ELEMENTARNI DOKAZ PRAŠTEVILSKEGA IZREKA

$$\pi(x) \sim \frac{x}{\log x}$$

Mentor:
dr.Aleksandar Jurišić

Kristijan Breznik
podiplomski študij
izobraževalna smer

Kazalo

POGLAVJE 1

Uvod

Delo je nastalo kot projekt pri predmetu Kriptografija in uvod v teorijo kodiranja, ki sem ga obiskoval pri prof. Jurišiću na FMF v Ljubljani v šolskem letu 2003/04. Praštevila imajo v kriptografiji posebno mesto in smo o njih veliko govorili, zato sem si izbral projekt povezan z njimi. Dolgo časa je bil težak in zanimiv problem koliko je približno praštevil do nekega poljubno velikega pozitivnega realnega števila. Namen naloge je elementaren dokaz praštevilskega izreka, ki nam odgovori na to vprašanje. Povejmo sedaj kaj imamo v mislih, ko govorimo o "elementarnem"dokazu. To pomeni, da ne uporabljamo kompleksne analize in si ne pomagamo z izreki iz analize, ampak uporabljamo samo osnovna dejstva iz teorije števil.

POGLAVJE 2

Zgodovina praštevilskega izreka

Praštevila so deležna pozornosti matematikov že od antike naprej. Veliko matematikov je iskalo formulo za število praštevil na poljubno velikih intervalih, a kljub velikim naporom dolgo časa niso uspeli narediti pomembnega koraka na tem področju. Tako se komaj konec 18. stoletja pojavi domneva, ki sta jo neodvisno drug od drugega razvila Gauss in Legendre. Pravilno sta domnevala, da je število praštevil do nekega realnega števila $x \geq 1$ približno enako $\frac{x}{\log x}$, kjer je z $\log x$ označen naravni logaritem števila x. Kljub temu, da se je Gauss problema lotil že v rani mladosti, pri petnajstih latih, svoje domneve ni uspel dokazati. To zgovorno priča o težavnosti našega problema.

Pol stoletja kasneje, na drugem koncu Evrope, je ruski matematik Chebyshev zapisal sploh prve dokaze o porazdelitvi praštevil. Med dokazi je vpeljal dve funkciji, ki sta v teoriji števil poznani kot funkciji Chebysheva in ju bomo spoznali v enem izmed naslednjih poglavij. Chebyshev je s svojim delom ogromno pripomogel k dokazu praštevilskega izreka.

Prvi dokaz praštevilskega izreka sta leta 1896 podala Hadamard in de la Vallée Poussin. Dokaz je vseboval splošno znano Riemannovo funkcijo zeta $\zeta(s)$. Ta funkcija je definirana kot absolutno konvergentna vrsta

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

za kompleksna števila s, ki imajo realni del večji od 1. Na tem mestu morda še enkrat povejmo kaj imamo v mislih, ko govorimo o "elementarnem"dokazu. V prvi vrsti to pomeni, da ne uporabljamo močnih izrekov analize kot je denimo Cauchyjev izrek, ampak samo osnovna dejstva o aritmetičnih funkcijah. Vsekakor v tem smislu prvi dokaz praštevilskega izreka ni bil elementaren.

Prelomnico v iskanju elementarnega dokaza praštevilskega izreka pomeni Hardyjevo predavanje iz leta 1921. Naš dokaz je primerjal s slavnim še vedno nerešenim problemom Riemannove zeta funkcije. Bil je zelo pesimističen glede nadalnjega iskanja elementarnega dokaza. Napovedal pa je, da se bo ob morebitnem uspehu marsikatera knjiga napisala na novo. Morda sta ravno ta govor in pričakovanja, ki so sledila, spodbudila matematike k še bolj zavzetemu delu. In tako je leta 1948, kmalu po drugi svetovni vojni, svet obšla novica, ki je šokirala matematično javnost. Erdös je objavil, da sta skupaj s Selbergom našla čisto elementaren dokaz praštevilskega izreka, ki temelji le na osnovnih lastnostih logaritemske funkcije. Toda na žalost je ravno ta objava privedla do nesoglasij med obema slavnima matematikoma. Ozadje vzrokov, ki so privedli do tega spora je zelo pestro in še vedno delno prikrito javnosti. Nedvomno je osnovo za dokaz postavil Selberg. Poimenoval jo je fundamentalna formula, v našem delu jo imenujemo Selbergova formula. Vendar

nikakor ni našel poti naprej. Le-to pa je hitro našel Erdös, ko mu je Selbergova formula slučajno prišla v roke. Po kratki izmenjavi mnenj in Erdösevi neuspešni pobudi za skupno delo sta potem kmalu dokaz dokončala vsak zase. Naj omenimo, da Selberg brez Erdösevega namiga zagotovo ne bi tako hitro uspel dokončati dokaza. Kljub temu je hotel dokaz zadržati zase, kar je kasneje tudi uradno uspel. Še več podrobnosti o tem dogajanju bralec lahko najde v Godfeld [**4**]. Za delo, ki sta ga opravila pri tem dokazu je Selberg leta 1950 prejel Fieldsovo medaljo, Erdös pa Coleovo nagrado dve leti kasneje.

Poudarimo še, da je naš dokaz že precej "izboljšana"verzija in seveda temu primerno krajša od originalnega dokaza.

POGLAVJE 3

Aritmetične funkcije in oznake

V drugem poglavju bomo najprej definirali pojem aritmetične funkcije in nato vpeljali nekaj aritmetičnih funkcij. Sledila bo predstavitev posebnega načina množenja funkcij, imenovanega Dirichletova konvolucija. Na koncu poglavja si bomo ogledali še nekaj oznak, ki bodo v naslednjih poglavjih nujno potrebne pri našem delu.

Pri dokazovanju praštevilskega izreka se bomo veliko ukvarjali s funkcijami, ki so definirane samo na množici naravnih števil. Takim funkcijam pravimo aritmetične funkcije. S praštevilskim izrekom je najbolj tesno povezana aritmetična funkcija Π, ki je definirana takole:

$$\Pi(n) = \begin{cases} 1; & n \text{ je praštevilo} \\ 0; & \text{sicer.} \end{cases}$$

Imenujemo jo tudi karakteristična funkcija praštevil. Med bolj preproste aritmetične funkcije sodijo še:

$$\delta(n) = \begin{cases} 1; & n = 1 \\ 0; & \text{sicer} \end{cases}$$

ter vse konstantne funkcije, ki zavzamejo isto konstanto za vsa naravna števila.
Podobno se obnaša

$$\ell(n) = \begin{cases} \log n; & n \text{ je praštevilo} \\ 0; & \text{sicer,} \end{cases}$$

ki jo bomo potrebovali v zadnjem poglavju. Naj bo $n = p_1^{r_1} \cdots p_k^{r_k}$ enolični razcep naravnega števila n na praštevila. Potem definiramo funkcijo ω na naslednji način:

$$\omega(n) = \begin{cases} 0; & n = 1 \\ k; & n = p_1^{r_1} \cdots p_k^{r_k}. \end{cases}$$

Naslednja aritmetična funkcija nima posebnega imena, a mi jo bomo potrebovali pri izreku Chebysheva, zato je prav, da jo omenimo že sedaj. Izberimo poljubno praštevilo p in pri vsakem naravnem številu n definirajmo $v_p(n)$ kot največje celo število r, za katerega velja $p^r | n$. Naj bo $v_p(n) = 0$ v primeru, ko praštevilo p naravnega števila n ne deli.
Seveda pa poznamo mnoge bolj zapleteno definirane aritmetične funkcije. Med drugimi bomo potrebovali Möbiousovo funkcijo

$$\mu(n) = \begin{cases} 1; & n = 1 \\ (-1)^k; & n \text{ je produkt } k \text{ različnih praštevil} \\ 0; & n \text{ deljiv s kvadratom večjim od 1} \end{cases}$$

in Von Mangoldtovo funkcijo

$$\Lambda(n) = \begin{cases} \log p; & n = p^k \text{ za neko praštevilo } p \text{ in } k \geq 1 \\ 0; & \text{sicer.} \end{cases}$$

Aritmetične funkcije najlažje seštevamo po točkah

$$(f + g)(n) = f(n) + g(n).$$

Množenje aritmetičnih funkcij definirajmo na naslednji način

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g(\tfrac{n}{d}) \tag{3.1}$$

in ga poimenujmo Dirichletova konvolucija. Množica vseh aritmetičnih funkcij s tako definiranima seštevanjem in množenjem funkcij nam tvori t.i. Dirichletov kolobar. Hitro se lahko prepričamo, da je Dirichletov kolobar komutativen kolobar z enoto δ. Komutativnost takoj sledi iz zapisa

$$(f * g)(n) = \sum_{dd'=n} f(d) \cdot g(d'),$$

ki je malo spremenjena formula (3.1). Za enoto je dovolj pokazati

$$(\delta * f)(n) = \sum_{d|n} \delta(d) \cdot f(\tfrac{n}{d}) = f(n),$$

kjer smo uporabili samo definicijo aritmetične funkcije δ.
Dirichletov kolobar ima mnoge lepe lastnosti. Nekatere, ki so pomembne za naše nadaljne delo, bomo tudi mi dokazali. Dogovorimo se glede zapisa. Z $f * g = h$ bomo na kratek način zapisali, da za vsak $n \in \mathbb{N}$ velja $(f * g)(n) = h(n)$.

Izrek 3.1. *Möbiousova funkcija μ in konstantna aritmetična funkcija* 1 *sta inverzni si funkciji v našem kolobarju.*

Dokaz. Radi bi pokazali naslednjo enakost

$$\mu * 1 = \delta.$$

Za $n = 1$ imamo $(\mu * 1)(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$.
V primeru, ko je $n \geq 2$ lahko enolično zapišemo $n = p_1^{r_1} \cdots p_k^{r_k}$. Zapis $m = p_1 \cdots p_k$ bomo imenovali radikal števila n. Ker 2 in višji eksponenti prispevajo 0 v vsoto, velja

$$(\mu * 1)(n) = \sum_{d|n} \mu(d) = \sum_{d|m} \mu(d).$$

Potem lahko nadaljujemo

$$\sum_{d|m} \mu(d) = \sum_{d|p_1 \cdots p_k} \mu(d) = \sum_{i=0}^{k} \sum_{\substack{d|n \\ \omega(d)=i}} (-1)^i.$$

Ker je m produkt k različnih praštevil, obstaja natanko $\binom{k}{i}$ deliteljev števila m, ki se dajo zapisati kot produkt i različnih praštevil, $0 \leq i \leq k$. Sledi

$$\sum_{i=0}^{k} \sum_{\substack{d|n \\ \omega(d)=i}} (-1)^i = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = \sum_{i=0}^{k} \binom{k}{i} (-1)^i \cdot 1^{k-i} = (-1+1)^k = 0.$$

□

Če Von Mangoldtovo funkcijo množimo z konstantno funkcijo 1, dobimo logaritemsko funkcijo. Tako imamo naslednji izrek:

Izrek 3.2. *V Dirichletovem kolobarju velja*

$$\Lambda * 1 = \log. \tag{3.2}$$

Dokaz. Če $n = 1$, potem $(\Lambda * 1)(1) = \Lambda(1) = 0 = \log 1$.
Naj bo zopet $n = p_1^{r_1} \cdots p_k^{r_k} \geq 2$. Velja

$$(\Lambda * 1)(n) = \sum_{d|n} \Lambda(d) = \sum_{i=1}^{k} \sum_{j=1}^{r_i} \Lambda(p_i^j) = \sum_{i=1}^{k} r_i \log p_i = \log n,$$

kar smo želeli pokazati.

□

Pomnožimo enačbo (3.2) z μ. Po izreku 3.1 na levi strani ostane samo Λ in tako dobimo naslednjo formulo $\Lambda = \mu * \log$. S pomočjo te formule lahko na naraven način definiramo posplošeno Von Mangoldtovo funkcijo, ki jo bomo potrebovali kasneje.

Definicija 3.3. *Za poljubno naravno število r lahko definiramo posplošeno Von Mangoldtovo funkcijo z naslednjo enačbo*

$$\Lambda_r = \mu * \log^r.$$

Izrek 3.4. *V Dirichletovem kolobarju velja*

$$\Lambda_2 = \Lambda \log n + \Lambda * \Lambda.$$

Dokaz. Množenje po točkah z logaritemsko funkcijo $\log(n)$ je odvajanje v našem kolobarju aritmetičnih funkcij. O tem si lahko več preberemo recimo v Bračič [**3**] na strani 36. Ker smo že prej pokazali, da velja $\log = 1 * \Lambda$, lahko izpeljemo

$$\begin{aligned} \log^2 &= \log \cdot \log \\ &= \log \cdot (1 * \Lambda) \\ &= 1 * (\log \cdot \Lambda) + (\log \cdot 1) * \Lambda \\ &= 1 * (\log \cdot \Lambda) + \log * \Lambda. \end{aligned}$$

Potem pa velja

$$\Lambda_2 = \mu * \log^2 = \mu * (1 * (\Lambda \cdot \log)) + \mu * (\log * \Lambda) = \Lambda \cdot \log + \Lambda * \Lambda.$$

□

Na začetku poglavja smo omenili aritmetično funkcijo Π, ki zavzame vrednost 1, če imamo opravka z naravnim številom, oziroma število 0 sicer. Definirajmo funkcijo $\pi(x) = \sum_{n \leq x} \Pi(n)$ za vsako realno število x. Funkcija π nam prešteje število praštevil, ki ne presegajo nekega realnega x. Že Evklid je znal pokazati, da obstaja neskončno praštevil. To bi lahko zapisali tudi takole:

$$\lim_{x \to \infty} \pi(x) = \infty.$$

Naša naloga je seveda še težja. Radi bi ugotovili koliko je praštevil med naravnimi števili. Izkaže se, da se za zelo velika števila $\pi(x)$ obnaša podobno kot funkcija $\frac{x}{\log x}$. Pri našem delu bomo imeli veliko opravka z ocenjevanjem funkcij, zato je prav, da se v tem poglavju dogovorimo za nekaj pojmov in oznak.

Definicija 3.5. *Naj bosta f in g kompleksni funkciji spremenljivke x, definirani na neki podmnožici realnih števil, ki vsebuje poljubno veliko število. Potem bomo rekli, da je funkcija f asimptotična funkciji g, ko gre $x \to \infty$, in pisali $f \sim g$, če je*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

Torej, praštevilski izrek nam pove, da je $\frac{x}{\log x}$ asimptotična funkcija za $\pi(x)$. Z drugimi besedami povedano velja $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1$. Srečali bomo še naslednji oznaki:

Definicija 3.6. *Naj bosta f in g kompleksni funkciji spremenljivke x, definirani na neki podmnožici realnih števil. Rekli bomo, da je funkcija f veliki O od g in pisali $f(x) = O(g(x))$, če obstaja taka konstanta C, da velja*

$$|f(x)| \leq C \cdot |g(x)| \text{ za vsak } x \text{ iz definicijskega območja.}$$

Za ilustracijo lahko navedemo, da je $x = O(x^2)$ za $x \geq 1$, saj lahko hitro najdemo tako konstanto, recimo $C = 1$, ki bo zadoščala pogoju iz definicije. Toda to ne velja na malo večjem območju, recimo za $x \geq 0$.

Definicija 3.7. *Naj bosta f in g kompleksni funkciji spremenljivke x, definirani na neki podmnožici realnih števil, ki vsebuje poljubno veliko število. Rekli bomo, da je funkcija f mali o od g, ko gre $x \to \infty$, in pisali $f(x) = o(g(x))$, če velja*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

Eden najbolj preprostih primerov je zopet $x = o(x^2)$, ki je na po zapisu čisto podoben primeru zgoraj, vendar se vseeno bistveno razlikuje.

Opomba 3.8. *Zadnje tri definicije so malce prilagojene našim potrebam. Bolj splošne verzije teh definicij si lahko preberete v Apostol* [**2**] *in Bračič* [**3**].

POGLAVJE 4

Funkciji Chebysheva

V veliko pomoč pri dokazovanju praštevilskega izreka nam bosta t.i. funkciji Chebysheva. Ime nosita po slavnem ruskem matematiku P. Chebyshevu, ki je pustil močan pečat v teoriji števil. Dokazali bomo izrek z njegovim imenom, ki je ob svojem nastanku pomenil sploh prvi dokaz na poti proti praštevilskemu izreku.

Funkciji Chebysheva sta definirani takole:

$$\vartheta(x) = \sum_{p \leq x} \log p$$

in

$$\psi(x) = \sum_{p^k \leq x} \log p.$$

Namen tega poglavja je pokazati, da je praštevilski izrek ekvivalenten $\vartheta(x) \sim x$, kar bomo s pridom uporabili v zadnjem poglavju.

Opomba 4.9. *Iz definicij obeh funkcij takoj sledi neenakost* $\vartheta(x) \leq \psi(x)$.

Trditev 4.10. *Za liho naravno število* n *velja*

$$\binom{n}{\frac{n+1}{2}} \leq 2^{n-1}. \tag{4.1}$$

Za sodo naravno število n *velja*

$$\binom{n}{\frac{n}{2}} \geq \frac{2^n}{n}. \tag{4.2}$$

Dokaz. Spomnimo se binomskega izreka:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Če vstavimo $a = b = 1$ dobimo

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \tag{4.3}$$

Naj bo sedaj n liho naravno število. Če v (4.3) zbrišemo vse koeficiente razen srednjih dveh dobimo

$$\binom{n}{\frac{n-1}{2}} + \binom{n}{\frac{n+1}{2}} \leq 2^n.$$

Ker velja

$$\binom{n}{\frac{n-1}{2}} = \frac{n!}{(n-\frac{n-1}{2})!(\frac{n-1}{2})!} = \frac{n!}{(\frac{n+1}{2})!(\frac{n-1}{2})!}$$

in

$$\binom{n}{\frac{n+1}{2}} = \frac{n!}{(n-\frac{n+1}{2})!(\frac{n+1}{2})!} = \frac{n!}{(\frac{n-1}{2})!(\frac{n+1}{2})!}$$

sta binomska koeficienta na levi enaka in lema za liha naravna števila drži. Pokažimo najprej, da če je n sod, je srednji binomski koeficient največji. Torej mora veljati:

$$\binom{n}{k-1} < \binom{n}{k} \iff k < \frac{n+1}{2}$$

in

$$\binom{n}{k-1} > \binom{n}{k} \iff k > \frac{n+1}{2}.$$

Ocenimo vrednost ulomka $\frac{\binom{n}{k}}{\binom{n}{k-1}}$.

$$\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{\frac{n!}{k!(n-k)!}}{\frac{n!}{(k-1)!(n-k+1)!}} = \frac{(k-1)!(n-k+1)!}{k!(n-k)!} = \frac{n-k+1}{k}$$

Ulomek je večji od 1 natanko tedaj, če $k < \frac{n+1}{2}$. Podobno je ulomek manjši od 1 natanko tedaj, če $k > \frac{n+1}{2}$. To dokazuje, da je za sode n srednji binomski koeficient res največji.

V vsoti imamo $n+1$ členov. Združimo prvega in zadnjega (dve enici) in dobimo n členov, ki so vsi manjši od srednjega člena. Sledi

$$n\binom{n}{\frac{n}{2}} \geq \sum_{k=0}^{n} \binom{n}{\frac{n}{k}} = 2^n.$$

□

Lema 4.11. *Naj bo $n \geq 2$ neko naravno število. Potem velja*

$$\prod_{p \leq n} p < 4^n.$$

Dokaz. Lemo dokažemo z indukcijo po n.
Za $n = 2$ imamo $2 < 4^2$, kar seveda drži.
Predpostavimo, da trditev velja za vsa naravna števila manjša od n. Ločimo dve možnosti. Če je n sod in večji od 2, potem seveda n ni praštevilo in po indukcijski predpostavki

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p < 4^{n-1} < 4^n.$$

Če je n lih lahko zapišemo $n = 2m+1$ za nek m iz množice naravnih števil. Oziroma $m = \frac{n-1}{2}$. Najprej razbijemo produkt na dva dela:

$$\prod_{p \leq n} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq n} p$$

Za prvi del uporabimo indukcijsko predpostavko. Opazimo tudi, da če je p praštevilo, ki zadošča $m+1 < p \leq n = 2m+1$, potem p deli produkt

$$(2m+1)2m(2m-1)(2m-2)\cdots(m+2),$$

vendar p ne deli $m!$. Iz tega sledi, da p deli $\binom{n}{m+1}$. Zato lahko zapišemo

$$\prod_{p\leq n} p < 4^{m+1} \cdot \binom{n}{m+1} \leq 4^{m+1}2^{n-1},$$

kjer smo si pri zadnjem neenačaju uporabili (4.1). Nato še malce uredimo in res dobimo

$$4^{m+1}2^{n-1} = 2^{2m+2}2^{2m} = 2^{4m+2} = 4^{2m+1} = 4^n.$$

□

Naslednjo trditev bomo podali brez dokaza. Dokaz trditve je elementaren in ga bralec lahko najde v Bračič [**3**].

Trditev 4.12. *(Legendrova enakost) Naj bo n poljubno naravno število in $n! = \prod_{p\leq n} p^{v_p(n!)}$ razcep števila $n!$ na potence različnih praštevil. Potem je*

$$v_p(n!) = \sum_{k=1}^{[\frac{\log n}{\log p}]} \left[\frac{n}{p^k}\right]. \tag{4.4}$$

□

Trditev 4.13. *Za vsako realno število x velja $[2x] - 2[x] \in \{0, 1\}$.*

Dokaz. Vsako realno število x lahko zapišemo v obliki $x = [x] + a$, kjer je $0 \leq a < 1$. Sledi $2x = 2[x] + 2a$. Ločimo dve možnosti:

(i) $0 < a < \frac{1}{2}$, dobimo $[2x] = 2[x]$,
(ii) $\frac{1}{2} \leq a < 1$, dobimo $[2x] = 2[x] + 1$.

□

Lema 4.14. *Za funkciji Chebysheva veljata naslednji neenakosti:*

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \leq \log 4 \tag{4.5}$$

in

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq \log 2. \tag{4.6}$$

Dokaz. Prva neenakost sledi takoj iz leme 4.11.
Za dokaz druge neenakosti bomo poiskali spodnjo mejo za funkcijo $\psi(x)$. Naj bo n poljubno naravno število in $N = \binom{2n}{n}$. Velja:

$$N = \binom{2n}{n} = \frac{(n+1)(n+2)\cdots 2n}{n!} = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{v_p((2n)!)-2v_p(n!)}.$$

Če uporabimo Legendrovo neenakost dobimo:

$$v_p((2n)!) - 2v_p(n!) = \sum_{k=1}^{[\frac{\log 2n}{\log p}]} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right) \leq \left[\frac{\log 2n}{\log p} \right],$$

kjer smo na koncu uporabili trditev 4.13.
S pomočjo tega, kar smo dobili in (4.2) lahko izpeljemo naslednje

$$\frac{2^{2n}}{2n} \leq N = \prod_{p \leq 2n} p^{v_p((2n)!) - 2v_p(n!)} \leq \prod_{p \leq 2n} p^{\left[\frac{\log 2n}{\log p} \right]}.$$

Po logaritmiranju imamo

$$2n \log 2 - \log 2n \leq \sum_{p \leq 2n} \left[\frac{\log 2n}{\log p} \right] \log p = \psi(2n).$$

Vzemimo sedaj $x \geq 2$ in $n = \left[\frac{x}{2} \right]$. Velja $2n \leq x \leq 2n + 2$ in

$$\psi(x) \geq \psi(2n) \geq 2n \log 2 - \log 2n > (x-2) \log 2 - \log x = x \log 2 - \log x - 2 \log 2.$$

Sledi

$$\liminf_{x \to \infty} \frac{\psi(x)}{x} \geq \log 2.$$

□

Pripravili smo vse potrebno za najpomembnejši izrek tega poglavja.

Izrek 4.15. *(Chebyshev) Obstajata takšni pozitivni konstanti, označimo ju z A in B, da velja*

$$Ax \leq \vartheta(x) \leq \psi(x) \leq \pi(x) \log x \leq Bx \tag{4.7}$$

za vse $x \geq 2$. Velja celo

$$\liminf_{x \to \infty} \frac{\vartheta(x)}{x} = \liminf_{x \to \infty} \frac{\psi(x)}{x} = \liminf_{x \to \infty} \frac{\pi(x) \log x}{x} \geq \log 2 \tag{4.8}$$

in

$$\limsup_{x \to \infty} \frac{\vartheta(x)}{x} = \limsup_{x \to \infty} \frac{\psi(x)}{x} = \limsup_{x \to \infty} \frac{\pi(x) \log x}{x} \leq \log 4. \tag{4.9}$$

Dokaz. Očitno iz (4.8) in (4.9) sledi (4.7). Pokažimo, da velja

$$\vartheta(x) \leq \psi(x) \leq \pi(x) \log x.$$

O prvi neenakosti smo se že pogovorjali, izpeljimo še drugo:

$$\psi(x) = \sum_{p^r \leq x} \log p = \sum_{p \leq x} \left(\sum_{p^r \leq x} 1 \right) \log p.$$

Če je $p^r \leq x$ in r naravno število je $r \leq [\frac{\log x}{\log p}]$. Seveda velja tudi obratno, zato lahko nadaljujemo

$$\sum_{p \leq x} \left(\sum_{p^r \leq x} 1 \right) \log p = \sum_{p \leq x} \left[\frac{\log x}{\log p} \right] \log p \leq \sum_{p \leq x} \log x = \pi(x) \log x.$$

Iz zgoraj povedanega takoj sledita neenakosti

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x}\leq\liminf_{x\to\infty}\frac{\psi(x)}{x}\leq\liminf_{x\to\infty}\frac{\pi(x)\log x}{x}$$

in

$$\limsup_{x\to\infty}\frac{\vartheta(x)}{x}\leq\limsup_{x\to\infty}\frac{\psi(x)}{x}\leq\limsup_{x\to\infty}\frac{\pi(x)\log x}{x}.$$

Sedaj bomo pokazali, da velja

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x}\geq\liminf_{x\to\infty}\frac{\pi(x)\log x}{x}\quad\text{in}\quad\limsup_{x\to\infty}\frac{\vartheta(x)}{x}\geq\limsup_{x\to\infty}\frac{\pi(x)\log x}{x},$$

nato upoštevali lemo 4.14 in izrek bo dokazan.
Za poljubno število $0<\delta<1$ velja

$$\vartheta(x)=\sum p\leq x\log p\geq\sum_{x^{1-\delta}<p\leq x}\log p\geq\sum_{x^{1-\delta}<p\leq x}\log x^{1-\delta}=(1-\delta)\log x\Bigg(\sum_{x^{1-\delta}<p\leq x}1\Bigg)=$$

$$=(1-\delta)\log x(\pi(x)-\pi(x^{1-\delta})\geq(1-\delta)\pi(x)\log x-x^{1-\delta}\log x.$$

Če delimo z x dobimo

$$\frac{\vartheta(x)}{x}\geq\frac{(1-\delta)\pi(x)\log x}{x}-\frac{\log x}{x^{\delta}}.$$

Ker $\frac{\log x}{x^{\delta}}\to 0$, ko $x\to\infty$, sledi

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x}\geq(1-\delta)\liminf_{x\to\infty}\frac{\pi(x)\log x}{x}$$

in

$$\limsup_{x\to\infty}\frac{\vartheta(x)}{x}\geq(1-\delta)\limsup_{x\to\infty}\frac{\pi(x)\log x}{x}.$$

Spomnimo se, da je bilo število $0<\delta<1$ poljubno, zato

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x}\geq\liminf_{x\to\infty}\frac{\pi(x)\log x}{x}$$

in

$$\limsup_{x\to\infty}\frac{\vartheta(x)}{x}\geq\limsup_{x\to\infty}\frac{\pi(x)\log x}{x}.$$

□

Iz izreka Chebysheva izhaja naslednja pomembna posledica.

Posledica 4.16. *Asimptotični formuli*

$$\vartheta(x)\sim x\quad in\quad\pi(x)\sim\frac{x}{\log x}\quad(x\to\infty)$$

sta ekvivalentni.

Dokaz. Če predpostavimo, da obstaja limita $\lim_{x\to\infty}\frac{\vartheta(x)}{x}$ in je enaka 1, potem po izreku Chebysheva sledi, da obstaja limita $\lim_{x\to\infty}\frac{\pi(x)\log x}{x}$ in je prav tako enaka 1. Podobno sklepamo tudi za obrat. □

POGLAVJE 5

Mertensove formule

Zdaj bomo pripravili orodja, ki jih bomo potrebovali v zadnjih dveh poglavjih. Najprej bomo definirali vsoto aritmetične funkcije in nato dokazali Abelovo enakost, ki bo zelo uporabna pri skoraj vseh dokazih v tem poglavju. Naslednji pomembnejši izrek bo izrek Mertensa, ki mu bo sledilo kar nekaj uporabnih posledic.

Izrek 5.17 (Abelova enakost). *Naj bosta $f(n)$ in $g(n)$ aritmetični funkciji. Definirajmo vsoto aritmetične funkcije*

$$F(x) = \sum_{n \leq x} f(n).$$

Če sta a in b naravni števili z lastnostjo $a < b$, potem velja

$$\begin{aligned} \sum_{n=a+1}^{b} f(n)g(n) &= F(b)g(b) - F(a)g(a+1) \\ &\quad - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)). \end{aligned}$$

Naj bosta x in y nenegativni realni števili in $[y] < [x]$. Če je $g(t)$ zvezno odvedljiva na intervalu $[y, x]$, potem velja

$$\sum_{y < n \leq x} f(n)g(n) = F(x)g(x) - F(y)g(y) - \int_y^x F(t)g'(t)dt.$$

Dokaz. Prvi del izreka preprosto izračunamo:

$$\begin{aligned} \sum_{n=a+1}^{b} f(n)g(n) &= \sum_{n=a+1}^{b} (F(n) - F(n-1))g(n) \\ &= \sum_{n=a+1}^{b} F(n)g(n) - \sum_{n=a}^{b-1} F(n)g(n+1) \\ &= F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)). \end{aligned}$$

Za drugi del uporabimo predpostavko, da je $g(t)$ zvezno odvedljiva na intervalu $[y, x]$. Potem je

$$g(n+1) - g(n) = \int_n^{n+1} g'(t)dt.$$

Ker za $n \leq t < n+1$ velja $F(t) = F(n)$, sledi

$$F(n)(g(n+1) - g(n)) = \int_n^{n+1} F(t)g'(t)dt.$$

Postavimo sedaj $a = [y]$ in $b = [x]$, da dobimo

$$\sum_{y<n\leq x} f(n)g(n) =$$

$$\begin{aligned}
&= F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)) \\
&= F(x)g(b) - F(y)g(a+1) - \sum_{n=a+1}^{b-1} \int_n^{n+1} F(n)(g(n+1) - g(n)) \\
&= F(x)g(x) - F(y)g(y) - F(x)(g(x) - g(b)) - F(y)(g(a+1) - g(y)) - \int_{a+1}^{b} F(t)g'(t)dt \\
&= F(x)g(x) - F(y)g(y) - \int_y^x F(t)g'(t)dt.
\end{aligned}$$

□

S pomočjo zgornjega izreka lahko izpeljemo nekaj krajših izrekov, ki jih bomo potrebovali pri svojem kasnejšem delu.

Izrek 5.18. *Za $x \geq 2$ velja*

$$\sum_{n\leq x} \log^2 n = x\log^2 x - 2x\log x + 2x + O(\log^2 x).$$

Dokaz. Uporabimo Abelovo enakost za $f(n) = 1$ in $g(t) = \log^2 t$. Velja $F(t) = [t]$ in $y'(t) = \frac{2\log t}{t}$. Tukaj se dogovorimo tudi za zapis

$$[x] = x - \{x\},$$

pri čemer bomo $\{x\}$ imenovali neceli del števila x. Zdaj lahko izpeljemo:

$$\begin{aligned}
\sum_{n\leq x} \log^2 n &= [x]\log^2 x - \int_1^x \frac{2\log t[t]}{t}dt \\
&= (x - \{x\})\log^2 x - 2\int_1^x \frac{(t - \{t\})\log t}{t}dt \\
&= x\log^2 x + O(\log^2 x) - 2\int_1^x \log t dt + 2\int_1^x \frac{\{t\}\log t}{t}dt \\
&= x\log^2 x - 2x\log x + 2x + O(\log^2 x).
\end{aligned}$$

□

Izrek 5.19. *Za $x \geq 2$ velja*

$$\sum_{n\leq x} \log^2 \frac{x}{n} = 2x + O(\log^2 x).$$

Dokaz. Izpeljimo

$$\begin{aligned}\sum_{n\le x}\log^2\frac{x}{n} &= \sum_{n\le x}(\log x-\log n)^2\\ &= \sum_{n\le x}(\log^2 x-2\log x\log n+\log^2 n)\\ &= [x]\log x-2\log x\sum_{n\le x}\log n-\sum_{n\le x}\log^2 n\\ &= x\log^2 x-2\log x(x\log x-x)+x\log^2 x-2x\log x+2x+O(\log^2 x)\\ &= 2x+O(\log^2 x),\end{aligned}$$

kjer smo zraven prejšnjega izreka uporabili še, da za $x\ge 2$ velja

$$\sum_{n\le x}\log n = x\log x-x+O(\log x).$$

Dokaz te zadnje formule je elementaren, a malce predolg, zato smo ga izpustili. Bralec ga lahko najde v Nathanson [**1**] na strani 208. □

Izrek 5.20. *Za $x\ge 1$ velja*

$$\sum_{n\le x}\frac{1}{n} = \log x\gamma + r(x),$$

kjer je

$$0<\gamma = 1-\int_1^\infty \frac{\{t\}}{t^2}dt<1$$

in

$$|r(x)|\le\frac{1}{x}.$$

Dokaz. Začnimo z oceno

$$0<\int_1^\infty\frac{\{t\}}{t^2}dt<\int_1^\infty\frac{1}{t^2}dt=1$$

in zato je $\gamma\in(0,1)$.
Sedaj ponovno uporabimo Abelovo enakost, izrek 5.17, za $f(n)=1$ in $g(t)=\frac{1}{t}$. Potem je $F(t)=\sum_{n\le t}1=[t]$. Sledi

$$\begin{aligned}\sum_{n\le x}\frac{1}{n} &= \sum_{n\le x}f(n)g(n)\\ &= \frac{[x]}{x}+\int_1^x\frac{[t]}{t^2}dt\\ &= 1-\frac{\{x\}}{x}+\int_1^x\frac{1}{t}dt-\int_1^x\frac{\{t\}}{t^2}dt\\ &= \log x+\left(1-\int_1^\infty\frac{\{t\}}{t^2}dt\right)+\int_1^\infty\frac{\{t\}}{t^2}dt-\frac{\{x\}}{x}\\ &= \log x+\gamma+r(x),\end{aligned}$$

kjer je

$$r(x) = \int_1^\infty \frac{\{t\}}{t^2} dt - \frac{\{x\}}{x}.$$

Ocenimo še

$$0 < \int_1^\infty \frac{\{t\}}{t^2} dt < \int_1^\infty \frac{1}{t} dt = \frac{1}{x}.$$

□

Izrek 5.21. *Velja*

$$\sum_{n \leq x} \frac{\mu(n)}{n} = O(1).$$

Dokaz. Po eni strani velja

$$\sum_{n \leq x} \mu(d) \left[\frac{x}{d}\right] = x \sum_{d \leq x} \mu(d) - \sum_{d \leq x} \mu(d) \left\{\frac{x}{d}\right\} = x \sum_{d \leq x} \mu(d) + O(x).$$

Lahko pa tudi izpeljemo

$$\sum_{n \leq x} \mu(d) \left[\frac{x}{d}\right] = \sum_{n \leq x} \sum_{d|n} \mu(d) = 1,$$

saj je

$$\sum_{dm \leq x} \mu(d) = \sum_{d \leq x} \mu(d) \sum_{n \leq \frac{x}{d}} 1 = \sum_{d \leq x} \mu(d) \left[\frac{x}{d}\right]$$

in

$$\sum_{dm \leq x} \mu(d) = \sum_{n \leq x} \sum_{d|n} \mu(d).$$

Če oboje združimo dobimo

$$x \sum_{d \leq x} \frac{\mu(d)}{d} + O(x) = 1$$

iz česar sledi

$$x \sum_{d \leq x} \frac{\mu(d)}{d} = O(x)$$

in

$$\sum_{d \leq x} \frac{\mu(d)}{d} = O(1).$$

□

Sedaj sledijo tako imenovani izreki Mertensa in njihove posledice.

Izrek 5.22 (Mertens). *Za $x \geq 1$ velja*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1)$$

in

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Dokaz. Najprej dokažimo prvo oceno. Podobno kot v prejšnjem dokazu je

$$\sum_{d\leq x}\Lambda(d)\left[\frac{x}{d}\right]=\sum_{n\leq x}\sum_{d|n}\Lambda(d)=\sum_{n\leq x}\log n=x\log x-x+O(\log x).$$

Zato lahko izpeljemo

$$\begin{aligned}x\log x-x+O(\log x) &= \sum_{d\leq x}\Lambda(d)\left[\frac{x}{d}\right]\\ &= \sum_{d\leq x}\Lambda(d)\left(\frac{x}{d}-\left\{\frac{x}{d}\right\}\right)\\ &= x\sum_{d\leq x}\frac{\Lambda(d)}{d}+\sum_{d\leq x}\Lambda(d)\left\{\frac{x}{d}\right\}\\ &= x\sum_{d\leq x}\frac{\Lambda(d)}{d}+O(\psi(x))\\ &= x\sum_{d\leq x}\frac{\Lambda(d)}{d}+O(x).\end{aligned}$$

Tako smo dobili

$$x\log x-x=x\sum_{d\leq x}\frac{\Lambda(d)}{d}+O(x).$$

Enačbo delimo z x in imamo

$$\sum_{d\leq x}\frac{\Lambda(d)}{d}=\log x+O(1).$$

Za dokaz druge ocene nadaljujemo

$$\begin{aligned}\sum_{n\leq x}\frac{\Lambda(n)}{n}-\sum_{p\leq x}\frac{\log p}{p} &= \sum_{\substack{p^k\leq x\\ k\geq 2}}\frac{\log p}{p^k}\\ &\leq \sum_{p\leq x}\log p\sum_{k=2}^{\infty}\frac{1}{p^k}\\ &\leq \sum_{p\leq x}\frac{\log p}{p(p-1)}=O(1).\end{aligned}$$

□

Izrek 5.23. *Za poljubno naravno število n velja*

$$\sum_{n\leq x}\frac{\vartheta(n)}{n^2}=\log x+O(1).$$

Dokaz. Najprej pokažimo, da je vrsta $\sum_{k\leq x}\frac{\ell}{k^2}$ konvergentna. Velja namreč

$$\sum_{k\leq x}\frac{\ell(k)}{k^2}\leq\sum_{k=1}^{\infty}\frac{\ell(k)}{k^2}<\sum_{k=1}^{\infty}\frac{\log k}{k^2}<\infty.$$

Z uporabo izreka 5.22 bomo izpeljali

$$\begin{aligned}
\sum_{n\le x}\frac{\vartheta(n)}{n^2} &= \sum_{n\le x}\sum_{k\le n}\frac{\ell(k)}{n^2}\\
&= \sum_{k\le n}\ell(k)\sum_{k\le n\le x}\frac{1}{n^2}\\
&= \sum_{k\le x}\ell(k)\left(\frac{1}{k}-\frac{1}{x}+O\left(\frac{1}{k^2}\right)\right)\\
&= \sum_{k\le x}\frac{\ell(k)}{k}-\frac{1}{x}\sum_{k\le x}\ell(k)+O\left(\sum_{k\le x}\frac{\ell(k)}{n^2}\right)\\
&= \sum_{p\le x}\frac{\log p}{p}+O(1)\\
&= \log x+O(1).
\end{aligned}$$

□

Izrek 5.24. *Obstaja taka konstanta B, da velja*

$$\sum_{p\le x}\frac{1}{p}=\log\log x+B+O\left(\frac{1}{\log x}\right).$$

Dokaz. Zapišimo $\sum_{p\le x}\frac{1}{p}$ v obliki

$$\sum_{p\le x}\frac{1}{p}=\sum_{p\le x}\frac{\log p}{p}\frac{1}{p}=\sum_{2\le n\le x}f(n)g(n),$$

kjer je

$$f(n)=\begin{cases}\frac{\log p}{p}; & \text{če je } n \text{ praštevilo,}\\ 0; & \text{sicer}\end{cases}$$

in

$$g(t)=\frac{1}{\log t}\quad \text{za } t\ge 1.$$

Definirajmo

$$F(t)=\sum_{n\le t}f(n)=\sum_{p\le t}\frac{\log p}{p}.$$

Potem je $F(t)=0$ za $t<2$. Po Mertensovem izreku 5.22 sledi

$$F(t)=\log t+r(t),\quad \text{kjer je } r(t)=O(1).$$

Zato integral

$$\int_2^\infty\frac{r(t)}{t\log^2 t}dt$$

konvergira absolutno in velja

$$\int_x^\infty\frac{r(t)}{t\log^2 t}dt=O\left(\frac{1}{\log x}\right).$$

Izračunajmo še integral $\int_2^y \frac{1}{x\log x}dx$, ki ga bomo potrebovali v spodnji oceni:

$$\int_2^y \frac{1}{x\log x}dx = \int_{\log 2}^{\log x} \frac{1}{t}dt = \log\log x - \log\log 2.$$

Sedaj lahko ob uporabi izreka 5.17 ocenimo

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} &= \sum_{n\le x} f(n)g(n)\\
&= F(x)g(x) - \int_2^x F(t)g'(t)dt\\
&= \frac{\log x + r(x)}{\log x} - \int_2^x \frac{\log t + r(t)}{t\log^2 t}dt\\
&= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}dt + \int_2^x \frac{r(t)}{t\log^2 t}dt\\
&= 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2 + \int_2^\infty \frac{r(t)}{t\log^2 t}dt - \int_x^\infty \frac{r(t)}{t\log^2 t}dt\\
&= \log\log x + B + O\left(\frac{1}{\log x}\right),
\end{aligned}$$

kjer je $B = 1 - \log\log 2 + \int_2^x \frac{r(t)}{t\log^2 t}dt$. □

Potrebovali bomo še tri leme

Lema 5.25. *Za $x \ge 2$ velja*

$$\int_2^x \frac{dt}{\log^2 t} = O\left(\frac{x}{\log^2 x}\right).$$

Dokaz. Razbijmo integral iz leme na dva dela:

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \le \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2\sqrt{x}}.$$

Sledi

$$\int_2^x \frac{dt}{\log^2 t} = O(\sqrt{x}) + O\left(\frac{x}{\log^2 x}\right) = O\left(\frac{x}{\log^2 x}\right),$$

saj je

$$\lim_{x\to\infty}\frac{\log^2 x}{\sqrt{x}} = 0.$$

□

Lema 5.26. *Velja*

$$\sum_{pq\le x}\frac{\log p\log q}{pq\log pq} = \log x + O(\log\log x),$$

kjer sta p in q praštevili.

Dokaz. Najprej pokažimo, da je

$$\begin{aligned}\sum_{pq\le x}\frac{\log p\log q}{pq} &= \sum_{p\le x}\frac{\log p}{p}\sum_{q\le\frac{x}{p}}\frac{\log q}{q}\\ &= \sum_{p\le x}\frac{\log p}{p}\Big(\log\frac{x}{p}+O(1)\Big)\\ &= \sum_{p\le x}\frac{\log p(\log x-\log p)}{p}+O\Big(\sum_{p\le x}\frac{\log p}{p}\Big)\\ &= \log x\sum_{p\le x}\frac{\log p}{p}-\sum_{p\le x}\frac{\log^2 p}{p}+O(\log x)\\ &= \log^2 x-\sum_{2\le n\le x}\frac{\ell(n)}{n}\log n+O(\log x).\end{aligned}$$

Srednji člen izračunamo s pomočjo Abelove vsote, torej izreka 5.17. Naj bo $f(n)=\frac{\ell(n)}{n}$ in $g(t)=\log t$. Potem je $F(t)=\sum_{n\le t}\frac{\ell(n)}{n}=\sum_{p\le t}\frac{\log p}{p}$. Sledi $F(t)=0$ za $t\ge 2$ in po izreku Mertensa

$$F(t)=\log t+r(t).$$

Ocenimo lahko

$$\int_2^\infty \frac{r)t)}{t}dt=O(\log x).$$

Po izreku 5.17 velja

$$\begin{aligned}\sum_{n\le x}\frac{\ell(n)}{n}\log n &= F(x)g(x)-\int_2^x F(t)g'(t)dt\\ &= (\log x+r(x))\log x-\int_2^x\frac{\log t+r(t)}{t}dt\\ &= \log^2 x+O(\log x)-\int_2^x\frac{\log t}{t}dt-\int_2^x\frac{r(t)}{t}dt\\ &= \log^2 x+O(\log x)-\frac{\log^2 x}{2}-\frac{\log^2 2}{2}-O(\log x),\end{aligned}$$

kjer smo upoštevali

$$\int_2^x\frac{r(t)}{t}dt=\int_2^\infty\frac{r(t)}{t}dt-\int_x^\infty\frac{r(t)}{t}dt=O(\log x).$$

Nadaljujmo z

$$\sum_{n\le x}\frac{\log p\log q}{pq\log pq}=\sum_{n\le x}\frac{\ell*\ell(n)}{n\log n}=\sum_{n\le x}\frac{\ell*\ell(n)}{n}\cdot\frac{1}{n}.$$

Podobno kot zgoraj uporabimo Abelovo enakost za

$$f(n)=\frac{\ell*\ell(n)}{n}$$

in

$$g(t) = \frac{1}{\log t}.$$

Potem je $F(t) = \sum_{n=pq\leq t} \frac{\log p \log q}{pq}$ za praštevila p, q. Imamo

$$\begin{aligned}
\sum_{n\leq x} \frac{\log p \log q}{pq \log pq} &= \left(\frac{1}{2}\log^2 x + O(\log x)\right)\frac{1}{\log x} - \int_2^x \frac{\frac{1}{2}\log^2 t + O(\log t)}{t\log^2 t}dt \\
&= \frac{1}{2}\log x + O(\log x) - \int_2^x \frac{1}{2t}dt - \int_2^x \frac{r(t)}{t\log^2 t}dt \\
&= \frac{1}{2}\log x + O(\log x) + \frac{1}{2}\log x + \frac{1}{2}\log 2 + O(\log\log x) \\
&= \log x + O(\log\log x).
\end{aligned}$$

□

Lema 5.27. *Za poljubno naravno število n velja*

$$\sum_{n\leq x} \frac{1}{1 + n\log n} = O(\log\log x).$$

Dokaz. Najprej opazimo, da velja

$$\sum_{n\leq x} \frac{1}{1+\log n} \leq \sum_{n\leq x} \frac{1}{\log n}.$$

Uporabimo Abelovo enakost za $f(n) = \frac{1}{n}$ in $g(t) = \frac{1}{\log t}$. Sledi $F(t) = \sum_{n\leq t} \frac{1}{n} = \log t + r(t)$, kjer je $r(t) = O(1)$.

$$\begin{aligned}
\sum_{n\leq x} \frac{1}{\log n} &= \sum_{n\leq x} f(n)g(n) \\
&= F(x)g(x) - \int_2^x F(t)g'(t)dt \\
&= \frac{\log x + r(x)}{\log x} - \int_2^x \frac{\log t + r(t)}{t\log^2 t}dt \\
&= 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2 + \int_2^\infty \frac{r(t)}{t\log^2 t}dt - \int_x^\infty \frac{r(t)}{t\log^2 t}dt \\
&= O(\log\log x).
\end{aligned}$$

□

POGLAVJE 6

Selbergova formula

Prvi konkretnejši korak proti dokazu praštevilskega izreka je formula, ki nosi ime po Atlu Selbergu. Namen tega poglavja je dokaz te formule. Selbeg jo je imenoval fundamentalna formula in jo nekaj časa ljubosumno skrival pred ostalimi matematiki. Vseeno je bil z njo seznanjen Erdös in lahko trdimo, da se je šele takrat pokazala vsa njena uporabnost.

Mnogokrat v teoriji števil se vsota aritmetične funkcije obnaša lepše kot funkcija sama. Tudi v Selbergovi formuli nastopa vsota ene izmed aritmetičnih funkcij in sicer posplošene Von Mangoldtove funkcije Λ_2.

Izrek 6.28 (Selbergova formula). *Za $x \geq 1$ velja*

$$\sum_{n\leq x} \Lambda_2(n) = 2x\log x + O(x). \tag{6.1}$$

Dokaz. Najprej s pomočjo osnovnih lastnosti posplošene Von Mangoldtove funkcije Λ_2 in Dirichletove konvolucije izpeljemo

$$\begin{aligned}\sum_{n\leq x}\Lambda_2(n) &= \sum_{n\leq x}\mu * \log^2(n)\\ &= \sum_{dk\leq x}\mu(d) * \log^2 k\\ &= \sum_{d\leq x}\mu(d)\sum_{k\leq \frac{x}{d}}\log^2 k,\end{aligned}$$

kjer d teče po vseh deliteljih števila n.
Uporabimo izrek 5.18

$$\begin{aligned}\sum_{n\leq x}\Lambda_2(n) &= \sum_{d\leq x}\mu(d)\sum_{k\leq\frac{x}{d}}\log^2 k,\\ &= \sum_{d\leq x}\mu(d)\left(\frac{x}{d}\log^2\frac{x}{d} - 2\frac{x}{d}\log\frac{x}{d} + 2\frac{x}{d} + O\left(\log^2\frac{x}{d}\right)\right)\\ &= x\sum_{d\leq x}\frac{\mu(d)}{d}\log\frac{x}{d}\left(\log\frac{x}{d} - 2\right) + 2x\sum_{d\leq x}\frac{\mu(d)}{d} + O\left(\sum_{d\leq x}\log^2\frac{x)}{d}\right).\end{aligned}$$

Za nadaljno oceno uporabimo izrek 5.19

$$\begin{aligned}\sum_{n\le x}\Lambda_2(n) &= x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\Big(\log\frac{x}{d}-2\Big)+2x\sum_{d\le x}\frac{\mu(d)}{d}+O\Big(\sum_{d\le x}\log^2\frac{x)}{d}\Big).\\ &= x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\Big(\log\frac{x}{d}-2\Big)+O(x).\end{aligned}$$

S pomočjo izreka 5.20 dobimo

$$\begin{aligned}\sum_{n\le x}\Lambda_2(n) &= x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\Big(\log\frac{x}{d}-2\Big)+O(x).\\ &= x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\Big(\sum_{m\le\frac{x}{d}}\frac{1}{m}-\gamma-2+O\Big(\frac{x}{d}\Big)\Big)+O(x)\\ &= x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\sum_{m\le\frac{x}{d}}\frac{1}{m}-(\gamma+2)x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}+O(x).\end{aligned}$$

Tako smo dobili dva člena v izrazu na desni strani zadnje enačbe, ki ju bomo ocenili vsakega posebej. Prvi člen nam da glavni del izraza na desni v Selbergovi formuli:

$$\begin{aligned}x\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}\sum_{m\le\frac{x}{d}}\frac{1}{m} &= x\sum_{dm\le x}\frac{\mu(d)}{dm}\log\frac{x}{d}\\ &= x\sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)\log\frac{x}{d}\\ &= x\log x\sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)-x\sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)\log d\\ &= x\log x+x\sum_{n\le x}\frac{\Lambda(n)}{n}\\ &= 2x\log x+O(x),\end{aligned}$$

saj je po Mertensovi formuli 5.22

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=x\log x+O(1).$$

Drugi člen ocenimo s ponovno uporabo izrekov 5.20 in 5.21:

$$\begin{aligned}\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d} &= \sum_{d\le x}\frac{\mu(d)}{d}\Big(\sum_{m\le\frac{x}{d}}\frac{1}{m}-\gamma+O\Big(\frac{x}{d}\Big)\Big)\\ &= \sum_{dm\le x}\frac{\mu(d)}{dm}-\gamma\sum_{d\le x}\frac{\mu(d)}{d}+O(1)\\ &= \sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)+O(1)=O(1).\end{aligned}$$

□

V dokazu praštevilskega izreka bomo potrebovali še naslednje ekvivalentne oblike prejšnjega izreka:

Izrek 6.29 (Selbergova formula). *Za $x\ge 1$ velja*

$$\sum_{p\le x}\log^2 p+\sum_{pq\le x}\log p\log q=2x\log x+O(x), \tag{6.2}$$

$$\vartheta(x)\log x+\sum_{p\le x}\log p\cdot\vartheta\Big(\frac{x}{p}\Big)=2x\log x+O(x), \tag{6.3}$$

$$\sum_{p\le x}\log p+\sum_{pq\le x}\frac{\log p\log q}{\log pq}=2x+O\Big(\frac{x}{1+\log x}\Big). \tag{6.4}$$

Dokaz. Po izreku 3.4 za vsak $n\in\mathbb{N}$ velja

$$\sum_{n\le x}\Lambda_2(n)=\sum_{n\le x}\Lambda(n)\log n+\sum_{n\le x}\Lambda*\Lambda(n).$$

Pobližje si oglejmo vsako vsoto posebej. Glede na definiranost Von Mangoldtove funkcije in lastnosti logaritmov za vse praštevilske potence p^k, ki delijo n velja

$$\begin{aligned}\sum_{n\le x}\Lambda(n)\log n &= \sum_{\substack{p^k\le x\\ k\ge 1}}\log^2 p^k\\ &= \sum_{\substack{p^k\le x\\ k\ge 1}}k\cdot\log^2 p\\ &= \sum_{p\le x}\log^2 p+\sum_{\substack{p^k\le x\\ k\ge 2}}k\cdot\log^2 p.\end{aligned}$$

V primeru, ko velja $p^k \leq x$ in $k \geq 2$, je $p \leq \sqrt{x}$ in zato

$$\begin{aligned}\sum_{\substack{p^k \leq x \\ k \geq 2}} k \cdot \log^2 p &= \sum_{p \leq \sqrt{x}} \log^2 p \sum_{k=2}^{[\frac{\log x}{\log p}]} k \\ &\leq \sum_{p \leq \sqrt{x}} \log^2 p \left(\frac{\log x}{\log p}\right)^2 \\ &\leq \sqrt{x} \cdot \log^2 x = O(x),\end{aligned}$$

kjer smo uporabili

$$\begin{aligned}\sum_{k=2}^{[\frac{\log x}{\log p}]} k &= \frac{[\frac{\log x}{\log p}] - 1}{2} \left(2 + [\frac{\log x}{\log p}]\right) \\ &\leq \frac{\left(\frac{\log x}{\log p}\right)^2}{2} + \left(\frac{\log x}{\log p}\right)^2 \\ &= \frac{\left(\frac{\log x}{\log p}\right)^2}{2} + \frac{\left(\frac{\log x}{\log p}\right)^2}{\left(\frac{\log x}{\log p}\right)} \\ &\leq \frac{\left(\frac{\log x}{\log p}\right)^2}{2} + \frac{\left(\frac{\log x}{\log p}\right)^2}{\left(\frac{\log x}{\frac{1}{2}\log x}\right)} \\ &= \frac{\left(\frac{\log x}{\log p}\right)^2}{2} + \frac{\left(\frac{\log x}{\log p}\right)^2}{2} \\ &= \left(\frac{\log x}{\log p}\right)^2.\end{aligned}$$

Zdaj bomo izračunali še drugo vsoto. Pisali bomo $n = uv$, kjer bo u tekel po vseh deliteljih števila n. Velja

$$\sum_{n \leq x} \Lambda * \Lambda(n) = \sum_{n \leq x} \sum_{n=uv} \Lambda(u)\Lambda(v).$$

Zaradi definicije Von Mangoldtove funkcije Λ nas zanimajo samo členi, kjer je u potenca nekega praštevila, prav tako mora biti tudi v potenca nekega praštevila. Torej samo členi oblike $n = uv = p^k q^l$ za neki praštevili p, q in naravni števili k, l.

Nadaljujemo

$$\begin{aligned}\sum_{n\leq x}\Lambda*\Lambda(n) &= \sum_{n\leq x}\sum_{n=uv}\Lambda(u)\Lambda(v)\\ &= \sum_{\substack{p^k\cdot q^l\leq x\\ k,l\geq 1}}\log p\log q\\ &= \sum_{pq\leq x}\log p\log q+\sum_{\substack{p^k\cdot q^l\leq x\\ k,l\geq 1,k+l\geq 3}}\log p\log q.\end{aligned}$$

S pomočjo izreka Chebysheva 4.15 bomo ocenili zadnji člen

$$\begin{aligned}\sum_{\substack{p^k\cdot q^l\leq x\\ k,l\geq 1,k+l\geq 3}}\log p\log q &\leq \sum_{\substack{p^k\cdot q^l\leq x\\ k\geq 2,l\geq 1}}\log p\log q+\sum_{\substack{p^k\cdot q^l\leq x\\ l\geq 2,k\geq 1}}\log p\log q\\ &= 2\sum_{\substack{p^k\cdot q^l\leq x\\ k\geq 2,l\geq 1}}\log p\log q\\ &= 2\sum_{\substack{p^k\leq x\\ k\geq 2}}\log p\sum_{\substack{q^l\leq \frac{x}{p^k}\\ l\geq 1}}\log q\\ &= 2\sum_{\substack{p^k\leq x\\ k\geq 2}}\log p\psi\left(\frac{x}{p^k}\right)\\ &= O\Big(\sum_{\substack{p^k\leq x\\ k\geq 2}}\frac{x\log p}{p}\Big)\\ &= O\Big(\sum_{p\leq x}\log p\sum_{k=2}^{\infty}\frac{1}{p^k}\Big)\\ &= O\Big(\sum_{p\leq x}\frac{\log p}{p(p-1)}\Big)\\ &= O(x).\end{aligned}$$

Imamo

$$\sum_{n\leq x}\Lambda*\Lambda(n)=\sum_{pq\leq x}\log p\log q+O(x).$$

Uporabimo izrek 6.28 in dobimo željeno

$$\begin{aligned}\sum_{n\leq x}\Lambda_2(n) &= \sum_{n\leq x}\Lambda(n)\log n+\sum_{n\leq x}\Lambda*\Lambda(n)\\ &= \sum_{p\leq x}\log^2 p+\sum_{pq\leq x}\log p\log q+O(x)\\ &= 2x\log x+O(x).\end{aligned}$$

Formula (6.2) je dokazana.
Najkrajši je dokaz (6.3). Na tem mestu se spomnimo aritmetične funkcije

$$l(n) = \begin{cases} \log n; & n \text{ je praštevilo} \\ 0; & \text{sicer.} \end{cases}$$

Velja

$$\vartheta(x) = \sum_{p \le x} \log p = \sum_{n \le x} \log n$$

in $\frac{\vartheta(x)}{x} = O(1)$ po izreku Chebysheva 4.15.
Z uporabo izreka 5.17 dobimo

$$\begin{aligned} \sum_{p \le x} \log^2 p &= \sum_{n \le x} l(n) \cdot \log n \\ &= \vartheta(x) \log x - \int_1^x \frac{\vartheta(t)}{t} dt \\ &= \vartheta(x) \log x + O(x). \end{aligned}$$

Tako imamo

$$\sum_{p \le x} \log^2 p = \vartheta(x) \log x + O(x). \tag{6.5}$$

Izpeljimo še

$$\sum_{pq \le x} \log p \log q = \sum_{p \le x} \log p \sum_{q \le \frac{x}{p}} \log q = \sum_{p \le x} \log p \cdot \vartheta\left(\frac{x}{p}\right). \tag{6.6}$$

Vstavimo (6.5) in (6.6) v (6.2) in dobimo (6.3).
Naj bo sedaj $f(n) = l(n) \log n + l * l(n)$. Formulo (6.2) lahko s pomočjo (6.3) zapišemo v obliki

$$\begin{aligned} F(x) &= \sum_{n \le x} f(n) \\ &= \sum_{n \le x} (l(n) \log n + l * l(n)) \\ &= \sum_{p \le x} \log^2 p + \sum_{pq \le x} \log p \log q \\ &= 2x \log x + O(x). \end{aligned}$$

Velja tudi $F(x) = 0$ za $x < 2$. Zopet uporabimo izrek 5.17 in imamo

$$\begin{aligned}\sum_{p\le x}\log p + \sum_{pq\le x}\log p\log q &= \sum_{2\le n\le x}\frac{l(n)\log n + l*l(n)}{\log n}\\ &= \sum_{\frac{3}{2}\le n\le x}\frac{f(n)}{\log n}\\ &= \frac{F(x)}{\log x} + \int_2 x\frac{F(t)}{t\log^2 t}dt\\ &= \frac{2x\log x + O(x)}{\log x} + \int_2 x\frac{2t\log t + O(t)}{t\log^2 t}dt\\ &= 2x + O\left(\frac{x}{\log x}\right),\end{aligned}$$

po lemi 5.25.
Če je $x \ge e$, potem je

$$\frac{x}{\log x} \le \frac{2x}{1+\log x}$$

in zato

$$O\left(\frac{x}{\log x}\right) \le O\left(\frac{x}{1+\log x}\right).$$

Za $1 \le x \le e$ je $\frac{x}{1+\log x} \ge 1$ in

$$0 \le \sum_{p\le x}\log p + \sum_{pq\le x}\frac{\log p\log q}{\log pq} \le \log 2.$$

Sledi

$$\begin{aligned}\left|x - \sum_{p\le x}\log p + \sum_{pq\le x}\frac{\log p\log q}{\log pq}\right| &= O(1)\\ &= O\left(\frac{x}{1+\log x}\right).\end{aligned}$$

□

POGLAVJE 7

Dokaz praštevilskega izreka

V zadnjem poglavju bomo dokazali praštevilski izrek. Uporabili bomo vse, kar smo si s trudom pripravili do sedaj.

Naj bo

$$R(x) = \vartheta(x) - x.$$

Pokažimo, da je dovolj dokazati $R(x) = o(x)$.

Trditev 7.30. *$\vartheta(x) \sim x$ je ekvivalentno $R(x) = o(x)$.*

Dokaz.
($\Longrightarrow$)
Vemo, da je $\vartheta(x) \sim x$ oziroma $\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$. Zato lahko izračunamo

$$\lim_{x\to\infty} \frac{R(x)}{x} = \lim_{x\to\infty} \frac{\vartheta(x) - x}{x} = \lim_{x\to\infty} \frac{\vartheta(x)}{x} - \lim_{x\to\infty} 1 = 1 - 1 = 0.$$

To pa ravno pomeni $R(x) = o(x)$.
($\Longleftarrow$)
Naj bo sedaj $\lim_{x\to\infty} \frac{R(x)}{x} = 0$. Potem je

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = \lim_{x\to\infty} \frac{\vartheta(x) - x + x}{x} = \lim_{x\to\infty} \frac{\vartheta(x) - x}{x} + 1 = 0 + 1 = 1$$

kar smo ravno želeli. □

Mi bomo torej v tem poglavju dokazali $R(x) = o(x)$, kar pa je po zgornji trditvi enakovredno praštevilskemu izreku. Bolj natančno, pokazali bomo, da obstajata zaporedji pozitivnih realnih števil $\{\delta_m\}_{m=1}^{\infty}$ in $\{u_m\}_{m=1}^{\infty}$ za kateri velja

$$\lim_{m\to\infty} \delta_m = 0$$

in

$$|R(x)| < \delta_m x \quad \text{za vsak } x \geq u_m.$$

Preden gremo na sam dokaz si bomo pripravili še nekaj rezultatov.

Lema 7.31. *Za $x > e$ velja*

$$\sum_{p\leq x} \frac{\log p}{p(1 + \log \frac{x}{p})} = O(\log\log x). \tag{7.1}$$

Dokaz. Vsoto po vseh praštevilih, ki so manjša ali enaka nekemu pozitivnemu realnemu x bomo razbili na intervale $(\frac{x}{e^j}, \frac{x}{e^{j-1}}]$ za $j = 1$ do $j = \log x$. Ker pa bomo seštevali le po celih številih bomo vzeli vsoto do $j = [\log x] + 1$. Torej lahko pišemo

$$\sum_{p \le x} \frac{\log p}{p(1 + \log \frac{x}{p})} = \sum_{j=1}^{[\log x]+1} \sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p(1 + \log \frac{x}{p})}$$

Vsak interval lahko po 5.22 ocenimo na naslednji način. Za vsako celo število j velja:

$$\begin{aligned} \sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p} &= \left(\log \frac{x}{e^{j-1}} + O(1)\right) - \left(\log \frac{x}{e^j} + O(1)\right) \\ &= \log \frac{x}{e^j} + \log e - \log \frac{x}{e^j} + O(1) \\ &= 1 + O(1) = O(1). \end{aligned}$$

Iz $\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}$ izpeljemo

$$\begin{array}{rcccl} \log \frac{x}{e^j} & < & \log p & \le & \log \frac{x}{e^{j-1}} \\ \log x - \log e^j & < & \log p & \le & \log x - \log e^{j-1} \\ \log x - j & < & \log p & \le & \log x - (j-1) \\ -j & < & \log p - \log x & \le & -(j-1) \\ j-1 & \le & \log x - \log p & < & j \\ j & \le & 1 + \log \frac{x}{p} & < & j+1. \end{array}$$

Sledi

$$\sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p(1 + \log \frac{x}{p})} \le \sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p \cdot j} = \frac{1}{j} \sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p} = O\left(\frac{1}{j}\right).$$

Zdaj lahko nadaljujemo

$$\sum_{j=1}^{[\log x]+1} \sum_{\frac{x}{e^j} < p \le \frac{x}{e^{j-1}}} \frac{\log p}{p(1 + \log \frac{x}{p})} = O\left(\sum_{j=1}^{[\log x]+1} \frac{1}{j}\right),$$

kar pa je po 5.24 enako $O(\log \log x)$. □

Izrek 7.32. *Za $x \ge 1$ velja*

$$|R(x)| \le \frac{1}{\log x} \sum_{n \le x} \left| R(\frac{x}{n}) \right| + O\left(\frac{x \log \log x}{\log x}\right).$$

Dokaz. Iz $R(x) = \vartheta(x) - x$ dobimo $\vartheta(x) = x + R(x)$ in to vstavimo v Selbergovo formulo (6.3):

$$\begin{aligned}
2x\log x + O(x) &= \vartheta(x)\log x + \sum_{p\le x}\log p\cdot\vartheta(\frac{x}{p}) \\
&= (x+R(x))\log x + \sum_{p\le x}\log p\left(\frac{x}{p}+R\left(\frac{x}{p}\right)\right) \\
&= x\log x + R(x)\log x + x\sum_{p\le x}\frac{\log p}{p} + \sum_{p\le x}R\left(\frac{x}{p}\right)\log p \\
&= R(x)\log x + \sum_{p\le x}R\left(\frac{x}{p}\right)\log p + 2x\cdot\log x + x\cdot O(1) \\
&= R(x)\log x + \sum_{p\le x}R\left(\frac{x}{p}\right)\log p + 2x\cdot\log x + O(x)
\end{aligned}$$

Na predzadnjem koraku smo uporabili izrek 5.22. Tako dobimo

$$R(x)\log x = -\sum_{p\le x}R\left(\frac{x}{p}\right)\log p + O(x). \tag{7.2}$$

Zdaj bomo poskusili $R(x)\log x$ izraziti še na drug način.
Naj bodo p, q, r praštevila in $p \le x$. Iz (6.4) sledi

$$\sum_{q\le\frac{x}{p}}\log q + \sum_{qr\le\frac{x}{p}}\frac{\log q\log r}{\log qr} = 2\frac{x}{p} + O\left(\frac{x}{p(1+\log\frac{x}{p})}\right).$$

Če zgornjo vrstico množimo z $\sum_{p\le x}\log p$ lahko izpeljem

$$\begin{aligned}
\sum_{p\le x}\log p\sum_{q\le\frac{x}{p}}\log q &= \sum_{pq\le x}\log p\log q \\
&= 2x\sum_{p\le x}\frac{\log p}{p} - \sum_{pqr\le x}\frac{\log p\log q\log r}{\log qr} + O\left(x\sum_{p\le x}\frac{\log p}{p(1+\log\frac{x}{p})}\right) \\
&= 2x(\log x + O(1)) - \sum_{qr\le x}\frac{\log q\log r}{\log qr}\cdot\sum_{p\le\frac{x}{qr}}\log p + O\left(x\sum_{p\le x}\frac{\log p}{p(1+\log\frac{x}{p})}\right) \\
&= 2x\log x - \sum_{qr\le x}\frac{\log q\log r}{\log qr}\cdot\vartheta\left(\frac{x}{qr}\right) + O(x\log\log x),
\end{aligned}$$

kjer smo v zadnji vrstici uporabili lemo 7.31. Dobili smo

$$\sum_{pq\le x}\log p\log q = 2x\log x - \sum_{qr\le x}\frac{\log q\log r}{\log qr}\cdot\vartheta\left(\frac{x}{qr}\right) + O(x\log\log x).$$

Spomnimo se Selbergove formule (6.2)

$$\sum_{p\le x}\log^2 p + \sum_{pq\le x}\log p\log q = 2x\log x + O(x).$$

V to Selbergovo formulo vstavimo zgornji izraz za $\sum_{pq\leq x}\log p\log q$ in dobimo

$$\sum_{p\leq x}\log^2 p=\sum_{pq\leq x}\frac{\log p\log q}{\log pq}\vartheta(\frac{x}{qr})+O(x\log\log x)$$

iz česar po definiciji funkcije ϑ takoj sledi

$$\vartheta(x)\log x=\sum_{pq\leq x}\frac{\log p\log q}{\log pq}\vartheta(\frac{x}{qr})+O(x\log\log x). \tag{7.3}$$

Zdaj zamenjajmo $\vartheta(x)$ z $x+R(x)$ in imamo

$$\begin{aligned}(x+R(x))\log x &= \sum_{pq\leq x}\frac{\log p\log q}{\log pq}\left(\frac{x}{qr}+R(\frac{x}{qr})\right)+O(x\log\log x)\\ &= x\sum_{pq\leq x}\frac{\log p\log q}{pq\log pq}+\sum_{pq\leq x}\frac{\log p\log q}{\log pq}R(\frac{x}{qr})+O(x\log\log x).\end{aligned}$$

Z uporabo leme 5.26 takoj dobimo

$$R(x)\log x=\sum_{pq\leq x}\frac{\log p\log q}{\log pq}R(\frac{x}{qr})+O(x\log\log x). \tag{7.4}$$

Seštejmo enačbi (7.3) in (7.4) in se spomnimo definicije ene izmed aritmetičnih funkcij iz drugega poglavja. Tako dobimo

$$\begin{aligned}2|R(x)|\log x &\leq \sum_{p\leq x}\log p\left|R(\frac{x}{p})\right|+\sum_{pq\leq x}\frac{\log p\log q}{\log pq}\left|R(\frac{x}{qr})\right|+O(x\log\log x)\\ &= \sum_{n\leq x}l(n)\left|R(\frac{x}{p})\right|+\sum_{n\leq x}\frac{l*l(n)}{\log n}\left|R(\frac{x}{n})\right|+O(x\log\log x).\end{aligned}$$

Morda še ni čisto vidno, ampak sedaj smo že zelo blizu cilja. V enačbi

$$2|R(x)|\log x=\sum_{n\leq x}l(n)\left|R(\frac{x}{p})\right|+\sum_{n\leq x}\frac{l*l(n)}{\log n}|R(\frac{x}{n})|+O(x\log\log x)$$

moramo oceniti še prvi člen na desni, nato pa bomo še vse skupaj delili z $2\log x$. Za oceno omenjenega izraza bomo uporabili izrek 5.17 za $a=0$ in $b=[x]$:

$$\sum_{n\leq x}f(n)g(n)=\sum_{n\leq x-1}F(n)\Big(g(n)-g(n+1)\Big)+F(x)g([x]).$$

Vzemimo

$$f(n)=l(n)+\frac{l*l(n)}{\log n}$$

in

$$g(n)=|R(\frac{x}{n})|.$$

Selbergovo formulo (6.4) lahko tokrat zapišemo v obliki

$$F(x)=\sum_{n\leq x}f(n)=\sum_{n\leq x}\left(l(n)+\frac{l*l(n)}{\log n}\right)=2x+O\left(\frac{x}{1+\log x}\right).$$

Če to vstavimo v zgoraj omenjeno parcialno vsoto dobimo enačbo

$$\sum_{n\le x}\left(l(n)+\frac{l*l(n)}{\log n}\right)\left|R\left(\frac{x}{n}\right)\right| = \sum_{n\le x-1}\left(2n+O\left(\frac{n}{1+\log n}\right)\right)\left(\left|R\left(\frac{x}{n}\right)\right|-\left|R\left(\frac{x}{n+1}\right)\right|\right)+ \tag{7.5}$$
$$+\left(2x+O\left(\frac{x}{1+\log x}\right)\right)\left|R\left(\frac{x}{[x]}\right)\right|.$$

Tako smo zgornji izraz v bistvu razbili na tri izraze, ki jih bomo ocenili vsakega posebej.
Z zadnjim je najmanj dela, zato začnimo kar z njim.

$$\left(2x+O\left(\frac{x}{1+\log x}\right)\right)\left|R\left(\frac{x}{[x]}\right)\right| = O(x),$$

saj sta oba člena v oklepaju $O(x)$. $\left|R(\frac{x}{[x]})\right| = O(1)$, saj je $1 \le \frac{x}{[x]} < 2$ za $x \ge 1$. Nadaljujmo z naslednjim členom desnega dela enačbe (7.5).

$$\begin{aligned} 2\sum_{n\le x-1} n\left(\left|R\left(\frac{x}{n}\right)\right|-\left|R\left(\frac{x}{n+1}\right)\right|\right) &= 2\sum_{n\le x-1} n\left(\left|R\left(\frac{x}{n}\right)\right|\right) - 2\sum_{n\le x-1} n\left(\left|R\left(\frac{x}{n+1}\right)\right|\right) \\ &= 2\sum_{n\le x-1} n\left(\left|R\left(\frac{x}{n}\right)\right|\right) - 2\sum_{2\le n\le x} (n-1)\left(\left|R\left(\frac{x}{n}\right)\right|\right) \end{aligned}$$

Oba dela razbijemo

$$2R(x) + 2\sum_{2\le n\le x-1} n\left(\left|R\left(\frac{x}{n}\right)\right|\right)-$$
$$-2\sum_{2\le n\le x-1}(n)\left(\left|R\left(\frac{x}{n}\right)\right|\right) + 2\sum_{2\le n\le x-1}\left(\left|R\left(\frac{x}{n}\right)\right|\right) - 2[x]\left|R\left(\frac{x}{[x]}\right)\right| =$$
$$= 2\sum_{n\le x}\left(\left|R\left(\frac{x}{n}\right)\right|\right) - 2[x]\left|R\left(\frac{x}{[x]}\right)\right| = 2\sum_{n\le x}\left(\left|R\left(\frac{x}{n}\right)\right|\right) + O(x),$$

saj je zopet $1 \le \frac{x}{[x]} < 2$ za $x \ge 1$ in zato $\left|R(\frac{x}{[x]})\right| = O(1)$.
Oceniti moramo še drugi člen. Najprej poglejmo razliko

$$\begin{aligned} \left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right| &= \left|\vartheta\left(\frac{x}{n}\right)-\frac{x}{n}\right| - \left|\vartheta\left(\frac{x}{n+1}\right)-\frac{x}{n+1}\right| \\ &\le \left|\vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)-\left(\frac{x}{n}-\frac{x}{n+1}\right)\right| \\ &\le \left|\vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)\right| + \left|\frac{x}{n}-\frac{x}{n+1}\right| \\ &= \vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)+\frac{x}{n}-\frac{x}{n+1} \\ &< \vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)+\frac{x}{n^2}, \end{aligned}$$

saj je

$$\frac{x}{n}-\frac{x}{n+1} = \frac{xn+x-xn}{n(n+1)} = \frac{x}{n^2+n} < \frac{x}{n^2} \quad \text{za } n>0.$$

Zato lahko pišemo

$$\sum_{n\le x-1}\left(\frac{n}{1+\log n}\right)\left(\left|R\left(\frac{x}{n}\right)\right|-\left|R\left(\frac{x}{n+1}\right)\right|\right)\le$$

$$\le\sum_{n\le x-1}\left(\frac{n}{1+\log n}\right)\left(\vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)\right)+x\sum_{n\le x-1}\frac{1}{n(1+\log n)}.$$

Ker je po lemi 5.27

$$\sum_{n\le x-1}\frac{1}{n(1+\log n)}=O(\log\log x),$$

bomo naprej ocenjevali le prvi del izraza. Podobno kot že enkrat prej bomo zamenjali spremenljivko po kateri seštevamo v eni izmed vsot:

$$\sum_{n\le x-1}\left(\frac{n}{1+\log n}\right)\left(\vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)\right)=$$

$$\begin{aligned}
&=\sum_{n\le x-1}\left(\frac{n}{1+\log n}\right)\vartheta\left(\frac{x}{n}\right)-\sum_{2\le n\le x}\left(\frac{n-1}{1+\log(n-1)}\right)\vartheta\left(\frac{x}{n}\right)\\
&=\vartheta(x)+\sum_{2\le n\le x-1}\left(\frac{n}{1+\log n}-\frac{n-1}{1+\log(n-1)}\right)\vartheta\left(\frac{x}{n}\right)\\
&\le\vartheta(x)+\sum_{2\le n\le x-1}\left(\frac{n}{1+\log n}-\frac{n-1}{1+\log n}\right)\vartheta\left(\frac{x}{n}\right)\\
&=\vartheta(x)+\sum_{2\le n\le x-1}\left(\frac{1}{1+\log n}\right)\vartheta\left(\frac{x}{n}\right)\\
&=O\left(x+x\sum_{2\le n\le x-1}\left(\frac{1}{n(1+\log n)}\right)\right)=O(x\log\log x),
\end{aligned}$$

po isti lemi kot zgoraj. Sedaj smo ocenili vse tri člene in lahko zapišemo

$$2|R(x)|\log x\le 2\sum_{n\le x}\left|R\left(\frac{x}{n}\right)\right|+O(x\log\log x).$$

Kot smo omenili že prej po deljenju z $2\log x$ dobimo željeni rezultat. □

Opomba 7.33. *Prejšnji izrek bi se lahko glasil tudi takole: za $x\ge 1$ velja*

$$|R(x)|\le\frac{1}{\log x}\sum_{n\le x}\left|R(\frac{x}{n})\right|+o(x). \tag{7.6}$$

Pred samim dokazom sledita še dve pripravljalni lemi.

Lema 7.34. *Naj bo $0>\delta<1$. Potem obstajata števili $c_0\ge 1$ in $x_1(\delta)\ge 4$, za kateri velja, da če je $x\ge x_1(\delta)$ potem obstaja naravno število n za katerega velja*

$$x<n\le e^{\frac{c_0}{\delta}}x$$

in

$$|R(n)| < \delta n.$$

Konstanta c_0 ni odvisna od δ.

Dokaz. Izrek 5.20 pravi

$$\sum_{n\le x}\frac{1}{n} = \log x + \gamma + r(x) = \log x + O(1),$$

kjer je $|r(x)| < \frac{1}{x}$. Iz tega lahko za $1 \le x < x'$ izpeljemo

$$\begin{aligned}\sum_{x<n\le x}\frac{1}{n} &= \sum_{n\le x'}\frac{1}{n} - \sum_{n\le x}\frac{1}{n}\\ &= \log x' + \gamma + r(x') - (\log x + \gamma + r(x))\\ &= \log x' - \log x + r(x') - r(x)\\ &= \log\frac{x'}{x} - r'(x),\end{aligned}$$

kjer je $|r'(x)| < \frac{2}{x}$, saj je

$$\left|\frac{1}{x'} - \frac{1}{x}\right| < \frac{1}{x} + \frac{1}{x} = \frac{2}{x}.$$

Po izreku 5.23 velja

$$\sum_{n\le x}\frac{\vartheta(n)}{n^2} = \log x + O(1)$$

in zato

$$\begin{aligned}\sum_{n\le x}\frac{R(n)}{n^2} &= \sum_{n\le x}\frac{\vartheta(n)-n}{n^2}\\ &= \sum_{n\le x}\frac{\vartheta(n)}{n^2} - \sum_{n\le x}\frac{1}{n^2}\\ &= \log x + O(1) - (\log x + O(1))\\ &= O(1).\end{aligned}$$

To nam da

$$\left|\sum_{x<n\le x'}\frac{R(n)}{n^2}\right| = O(1)$$

za vsak $1 \le x < x'$. Z drugimi besedami povedano je izraz na desni strani zgornje enačbe omejen. Torej lahko izberemo tak $c_0 \ge 1$, da bo veljalo

$$\left|\sum_{x<n\le x'}\frac{R(n)}{n^2}\right| < \frac{c_0}{2} \tag{7.7}$$

za vsak $1 \le x < x'$.

Naj bo $\frac{c_0}{\delta} > 1$ in $\rho = e^{\frac{c_0}{\delta}}$. Ker je $x \ge 1$ je $\rho x > ex$. Izberimo tak $x_1(\delta) \ge 4$, da bo $\log x < \delta x$ za

vsak $x \geq x_1(\delta)$. Pokazali bi radi, da če je $x \geq x_1(\delta)$ potem obstaja naravno število $n \in (x, \rho x]$ za katerega je $|R(n)| < \delta$.
Ločimo dva primera.

(i) Predpostavimo, da je bodisi $R(n) \geq 0$ za vsako naravno število $n \in (x, \rho x]$ bodisi $R(n) \leq 0$ za vsako naravno število $n \in (x, \rho x]$. Potem velja

$$\left| \sum_{x<n\leq \rho x} \frac{R(n)}{n^2} \right| = \sum_{x<n\leq \rho x} \frac{|R(n)|}{n^2} = \sum_{x<n\leq \rho x} \left(\frac{R(n)}{n}\right)\frac{1}{n}.$$

Označimo z

$$m^* = \min\left\{ \frac{|R(x)|}{n}; n \in n \in (x, \rho x] \right\}.$$

Spomnimo se kako smo izbrali c_0 v (7.7). Sedaj lahko nadaljujemo

$$\begin{aligned} \frac{c_0}{2} &> \sum_{x<n\leq \rho x} \left(\frac{R(n)}{n}\right)\frac{1}{n} \\ &\geq m^* \sum_{x<n\leq \rho x} \frac{1}{n} \\ &> m^*\left(\log\frac{\rho x}{x} - \frac{2}{x} \right) \\ &\geq m^*\left(\log\frac{c_0}{\delta} - \frac{1}{2} \right) \\ &\geq \frac{c_0 m^*}{2\delta}. \end{aligned}$$

Sledi

$$0 \leq m^* < \delta.$$

Ker obstaja naravno število $n \in (x, \rho x]$ z lastnostjo $\frac{|R(n)|}{n} = m^*$ je $|R(n)| < \delta n$.

(ii) Recimo, da obstajata dve naravni števili na intervalu $(x, \rho x]$ za kateri velja $R(n-1) \neq R(n)$ in $R(n-1)R(n) \leq 0$. Iz $n - 1 > x \geq x_1(\delta) \geq 4$ sledi $n \geq 6$. Po drugi strani za vsako naravno število $n \geq 2$ velja

$$\begin{aligned} R(n) - R(n-1) &= \vartheta(n) - \vartheta(n-1) - 1 \\ &= \sum_{p\leq n} \log p - \sum_{p\leq n-1} \log p - 1 \\ &= \begin{cases} \log n - 1; & \text{če je n praštevilo} \\ -1; & \text{sicer.} \end{cases} \end{aligned}$$

Če je $R(n) < R(n-1)$, potem je razlika $R(n) - R(n-1)$, zaradi velikosti $n-$ja, enaka -1. Ker pa velja tudi $R(n) \leq 0 \leq R(n-1)$, je $|R(n)| \leq 1 < \log n \leq \delta n$, kar smo želeli. Podobno, če je $R(n-1) < R(n)$, sledi $R(n-1) \leq 0 \leq R(n)$ in

$$0 \leq R(n) \leq R(n) - R(n-1) = \log n - 1 < \log n < \delta n.$$

Prepričali smo se, da v vseh primerih obstaja naravno število $n \in (x, \rho x]$, z lastnostjo

$$|R(n)| < \delta n.$$

□

Lema 7.35. *Naj bo $c_0 \geq 1$ število, ki smo ga skonstruirali v lemi 7.34 in naj bo $0 < \delta < 1$. Potem obstaja tako število $x_2(\delta)$, da v primeru, ko je $x \geq x_2(\delta)$ interval $(x, e^{\frac{c_0}{\delta}}x]$ vsebuje tak podinterval $(y, e^{\frac{c_0}{\delta}}y]$, da velja*

$$|R(t)| < 4\delta t$$

za vsak $t \in (y, e^{\frac{c_0}{\delta}}y]$.

Dokaz. Zopet uporabimo Selbergovo formulo (6.4). Za $x \geq 1$ velja

$$\sum_{p \leq n} \log p + \sum_{pq \leq n} \frac{\log p \log q}{\log pq} = 2x + O\left(\frac{x}{1 + \log x}\right).$$

S pomočjo te formule lahko za $1 < u \leq t$ izpeljemo

$$\begin{aligned} 0 &\leq \sum_{u < p \leq t} \log p \\ &\leq \sum_{u < p \leq t} \log p + \sum_{u < p \leq t} \frac{\log p \log q}{\log pq} \\ &= 2t + O\left(\frac{t}{1 + \log t}\right) - 2u - O\left(\frac{u}{1 + \log u}\right) \\ &= 2(t - u) + O\left(\frac{t}{1 + \log t}\right), \end{aligned}$$

ker je funkcija $\frac{t}{1+\log t}$ naraščajoča za $t \geq 1$. Velja pa tudi

$$\sum_{u < p \leq t} \log p = \vartheta(t) - \vartheta(u) = R(t) + t - R(u) - u = t - u + R(t) - R(u).$$

Iz obojega lahko zapišemo neenakost

$$-(t - u) \leq R(t) - R(u) \leq t - u + O\left(\frac{t}{1 + \log t}\right).$$

Seveda za $1 < u \leq t$ takoj sledi

$$|R(t) - R(u)| \leq t - u + O\left(\frac{t}{1 + \log t}\right) \leq t - u + O\left(\frac{t}{\log t}\right).$$

Če je $1 < t \leq u \leq 2t$, potem

$$\begin{aligned} |R(t) - R(u)| &\leq u - t + O\left(\frac{u}{1+\log u}\right) \\ &\leq |t-u| + O\left(\frac{2t}{1+\log 2t}\right) \\ &\leq |t-u| + O\left(\frac{t}{\log t}\right). \end{aligned}$$

Mi bomo potrebovali posebni primer, ko je $u \geq 4$ in $\frac{t}{2} \leq u \leq t$:

$$|R(t)| \leq |R(u)| + |t-u| + O\left(\frac{t}{\log t}\right). \tag{7.8}$$

Po lemi 7.34 obstaja tako število $c_0 \geq 1$, da za $0 < \delta < 1$ in $x \geq x_1(\delta) \geq 4$ obstaja naravno število

$$n \in (x, e^{\frac{c_0}{\delta}} x]$$

in

$$|R(n)| < \delta n.$$

Če je t realno število iz intervala $[\frac{n}{2}, 2n]$, potem $\frac{t}{2} \leq n \leq 2t$. Ker pa je $n > x \geq 4$ imamo

$$\log t \geq \log(\frac{n}{2}) > \log(\frac{x}{2}) \geq \frac{\log x}{2}.$$

Nato lahko ocenimo

$$\begin{aligned} |R(t)| &\leq |R(n)| + |t-n| + O\left(\frac{t}{\log t}\right) \\ &< \delta n + |t-n| + O\left(\frac{t}{\log x}\right) \\ &= t\left(\frac{\delta n}{t} + \left|\frac{t}{n} - 1\right| + O\left(\frac{1}{\log x}\right)\right) \\ &= t\left(2\delta + \left|\frac{t}{n} - 1\right| + O\left(\frac{1}{\log x}\right)\right). \end{aligned}$$

Kar pomeni, da je $t\left(2\delta + \left|\frac{t}{n} - 1\right| + \frac{c_2}{\log x}\right)$, za neko konstanto c_2.
Za $x \geq x_2(\delta) = \max(x_1(\delta), e^{\frac{c_0}{\delta}})$ je

$$|R(t)| < t\left(3\delta + \left|\frac{t}{n} - 1\right|\right).$$

Izberimo t, da bo veljalo

$$e^{-\frac{\delta}{2}} n \leq t \leq e^{\frac{\delta}{2}} n.$$

Potem je $t \in (\frac{n}{2}, 2n)$, saj je $e^{\frac{\delta}{2}} < e^{\frac{1}{2}} < 2$.
Če je $\frac{t}{n} \geq 1$, potem je $\left|\frac{t}{n} - 1\right| = \frac{t}{n} - 1 \leq e^{\frac{\delta}{2}} - 1 < \delta$, saj je $e^{\frac{\delta}{2}} < 1 + \delta$ za $0 < \delta < 1$.
Če pa je $\frac{t}{n} < 1$, potem je $\left|\frac{t}{n} - 1\right| = 1 - \frac{t}{n} < 1 - e^{-\frac{\delta}{2}} < e^{\frac{\delta}{2}} - 1 < \delta$. Ker je v obeh primerih $\left|\frac{t}{n} - 1\right| < \delta$ imamo

$$|R(t)| < 4\delta t.$$

Sedaj definirajmo število y na naslednji način.
Če je $e^{\frac{\delta}{2}} n \leq e^{\frac{c_0}{\delta}} x$, naj bo $y = n$.
Če pa je $e^{\frac{\delta}{2}} n > e^{\frac{c_0}{\delta}} x$, naj bo $y = e^{-\frac{\delta}{2}} n$. V drugem primeru sledi

$$y = e^{-\frac{\delta}{2}} n = e^{-\delta + \frac{\delta}{2}} n > e^{-\delta} \cdot e^{\frac{c_0}{\delta}} \cdot x = e^{\frac{c_0}{\delta} - \delta} x,$$

ker je $\frac{c_0}{\delta} > c_0 \geq 1 > \delta$.
V obeh primerih velja

$$(y, e^{\frac{\delta}{2}} y] \subset (x, e^{\frac{c_0}{\delta}} x]$$

in

$$|R(t)| < 4\delta t$$

za vsak $t \in (y, e^{\frac{\delta}{2}} y]$. □

Končno smo se dokopali do samega praštevilskega izreka.

Izrek 7.36 (Praštevilski izrek). *Za Chebyshevo funkcijo $\vartheta(x)$ velja*

$$\vartheta(x) \sim x,$$

ko pošljemo $x \to \infty$.

Dokaz. Po lemi 4.11 in lemi 4.14 sledita naslednji neenakosti

$$\limsup_{x \to \infty} \frac{R(x)}{x} = \limsup_{x \to \infty} \frac{\vartheta(x)}{x} - 1 \leq \log 4 - 1 < 0,4$$

in

$$\liminf_{x \to \infty} \frac{R(x)}{x} = \liminf_{x \to \infty} \frac{\vartheta(x)}{x} - 1 \geq \log 2 - 1 < -0,4.$$

Kar pomeni, da je funkcija $\frac{|R(x)|}{x}$ omejena oziroma celo

$$\lim_{x \to \infty} \frac{|R(x)|}{x} < 0,4.$$

Torej obstajata števili M in u_1, da je

$$|R(x)| \leq Mx \quad \text{za vsak } x \geq 1$$

in

$$|R(x)| \leq \delta_1 x \quad \text{za vsak } x \geq u_1,$$

kjer je $\delta_1 = 0,4$.
Naša naloga bo induktivno skonstruirati takšni zaporedji realnih števil $\{\delta_m\}_{m=1}^{\infty}$ in $\{\varepsilon_m\}_{m=1}^{\infty}$, da bo veljalo

$$\delta_1 > \delta_2 > \delta_3 \cdots$$

in

$$\lim_{m\to\infty} \varepsilon_m = 0. \tag{7.9}$$

Naj bo $m \geq 1$ in recimo, da smo že določili δ_m. Naj bo c_0 število iz leme 7.34. Izberimo ε_m, da bo veljalo $0 < \varepsilon_m < \frac{1}{m}$ in

$$(1+\varepsilon_m)\left(1 - \frac{\delta_m^2}{256c_0}\right) < 1.$$

Zdaj definirajmo

$$\delta_{m+1} = (1+\varepsilon_m)\left(1 - \frac{\delta_m^2}{256c_0}\right)\delta_m. \tag{7.10}$$

Zagotovo velja $0 < \delta_{m+1} < \delta_m$.
V naslednjem delu dokaza bomo pokazali, da za vsak m obstaja tako število u_m, da velja

$$|R(x)| \leq \delta_m x \quad \text{za vsak } x \geq u_m. \tag{7.11}$$

Pokažimo, da je to res dovolj za dokaz praštevilskega izreka. Zaporedje $\{\delta_m\}_{m=1}^{\infty}$ je strogo padajoče zaporedje pozitivnih realnih števil. Vemo, da imajo taka zaporedja limito in da je ta limita nenegativno število, označimo ga z $\delta < 1$. S pomočjo leme 7.9 in leme 7.10 sledi

$$\begin{aligned}
\lim_{m\to\infty} \delta_{m+1} &= \lim_{m\to\infty} (1+\varepsilon_m)\left(1 - \frac{\delta_m^2}{256c_0}\right)\delta_m \\
\delta &= \left(1 - \frac{\delta^2}{256c_0}\right)\delta \\
\delta\left(1 - 1 + \frac{\delta^2}{256c_0}\right) &= 0 \\
\delta^2 &= 0 \\
\delta &= 0.
\end{aligned}$$

Kar pa pomeni, da je za velike $m-$ je $\frac{|R(x)|}{x}$ poljubno majhno pozitivno število oziroma $R(x) = o(x)$.
Preostane nam še konstrukcija števila u_m. Tudi to število bomo določili induktivno. Na začetku dokaza smo že videli, da obstaja u_1, da velja $|R(x)| \leq \delta_1 x \quad$ za vsak $x \geq u_1$. Pa recimo, da smo že našli u_m. Pokazali bi radi, da obstaja u_{m+1}, da velja $|R(x)| \leq \delta_{m+1} x \quad$ za vsak $x \geq u_{m+1}$.
Definirajmo $\delta'_m = \frac{\delta_m}{8}$ in $\rho = e^{\frac{c_0}{\delta_m}}$. Naj bo $x_2(\delta'_m)$ število konstruirano v lemi 7.35 in naj bo

$$x_3(m) = \max(x_2(\delta' m), u_m).$$

Če je $x \geq x_3(m) \geq x_2(\delta' m)$, potem po lemi 7.35 vsak interval $(x, \rho x]$ vsebuje tak podinterval $(y, e^{\frac{\delta'_m}{2}} y]$, da je

$$|R(t)| < 4\delta'_m t = \frac{\delta_m t}{2}$$

za vsak $t \in (y, e^{\frac{\delta'_m}{2}} y]$. Naj bo nato k največje celo število, da velja $\rho^k \leq \frac{x}{x_3(m)}$. Izpeljemo lahko

$$\begin{aligned} k &\leq \frac{\log \frac{x}{x_3(m)}}{\log \rho} < k+1 \\ k &= \frac{\log \frac{x}{x_3(m)}}{\log \rho} + O(1) \\ &= \frac{\delta'_m \log \frac{x}{x_3(m)}}{c_0} + O(1) \\ &= \frac{\delta'_m \log x}{c_0} - \frac{\delta'_m \log x_3(m)}{c_0} + O(1) \\ &\leq \frac{\delta_m \log x}{8c_0} + O(1). \end{aligned}$$

S pomočjo izreka 7.32 ocenimo

$$\begin{aligned} |R(x)| &\leq \frac{1}{\log x} \sum_{n \leq x} \left| R\left(\frac{x}{n}\right) \right| + o(x) \\ &= \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + \frac{1}{\log x} \sum_{\rho^k < n \leq x} \left| R\left(\frac{x}{n}\right) \right| + o(x) \\ &= \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + \frac{x}{\log x} \sum_{\rho^k < n \leq x} \left| R\left(\frac{1}{n}\right) \right| + o(x) \end{aligned}$$

Sedaj uporabimo začetek dokaza, ko smo ugotovili, da obstaja tako število M, da velja

$$\left| R\left(\frac{x}{n}\right) \right| < M\frac{x}{n} = Mx\frac{1}{n},$$

za vsak $\frac{x}{n} \geq 1$ oziroma $x \geq n$. Tako lahko nadaljujemo

$$\begin{aligned} |R(x)| &= \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + \frac{x}{\log x} \sum_{\rho^k < n \leq x} \left| R\left(\frac{1}{n}\right) \right| + o(x) \\ &\leq \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + \frac{Mx}{\log x} \sum_{\rho^k < n \leq x} \frac{1}{n} + o(x) \\ &\leq \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + o(x), \end{aligned}$$

kjer smo za oceno $\sum_{\rho^k < n \leq x} \frac{1}{n}$ uporabili izrek 5.20.
V naslednjem delu dokaza bomo poskušali oceniti še prvi člen na desni strani zgornje neenakosti.

Za $1 \leq n \leq \rho^k$ je

$$\frac{x}{n} \geq \frac{x}{\rho^k} \geq x_3(m) \geq u_m$$

iz česar sledi

$$\left|R\left(\frac{x}{n}\right)\right| < \delta_m \frac{x}{n} \tag{7.12}$$

po predpostavki za u_m.
Za $j = 1, \ldots, k$ imamo

$$\frac{x}{\rho^j} \geq \frac{x}{\rho^k} \geq x_3(m) \geq x_2(\delta'_m)$$

in zato po lemi 7.35 interval $(\frac{x}{\rho^j}, \frac{x}{\rho^j - 1}]$ vsebuje tak podinterval $I_j = (y_j, e^{\frac{\delta'_m}{2}} y_j]$, da velja

$$\left|R(t)\right| < 4\delta'_m t = \frac{\delta_m t}{2} \quad \text{za vsak } t \in I_j. \tag{7.13}$$

S pomočjo neenakosti (7.12) in (7.13) lahko ocenimo

$$\begin{aligned}
\sum_{n \in (\rho^{j-1}, \rho^j]} \left|R\left(\frac{x}{n}\right)\right| &= \sum_{n \in (\rho^{j-1}, \rho^j] \setminus I_j} \left|R\left(\frac{x}{n}\right)\right| + \sum_{n \in I_j} \left|R\left(\frac{x}{n}\right)\right| \\
&< \delta_m x \sum_{n \in (\rho^{j-1}, \rho^j] \setminus I_j} \frac{1}{n} + \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n} \\
&= \delta_m x \sum_{n \in (\rho^{j-1}, \rho^j]} \frac{1}{n} - \delta_m x \sum_{n \in I_j} + \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n} \\
&= \delta_m x \sum_{n \in (\rho^{j-1}, \rho^j]} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n}.
\end{aligned}$$

Tako lahko nadaljujemo

$$\begin{aligned}
\sum_{n \leq \rho^k} \left|R\left(\frac{x}{n}\right)\right| &= R(x) + \sum_{j=1}^{k} \sum_{n \in (\rho^{j-1}, \rho^j]} \left|R\left(\frac{x}{n}\right)\right| \\
&\leq \delta_m x + \sum_{j=1}^{k} \left(\delta_m x \sum_{n \in (\rho^{j-1}, \rho^j]} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n} \right) \\
&= \delta_m x \sum_{n \leq \rho^k} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{j=1}^{k} \sum_{n \in I_j} \frac{1}{n}.
\end{aligned}$$

Za prvi člen uporabimo izrek 5.20

$$\begin{aligned}\delta_m x \sum_{n\le\rho^k}\frac{1}{n} &= \delta_m x(\log\rho^k + O\Big(\frac{1}{\rho^k}\Big)\\ &= \delta_m x k\log\rho + O\Big(\frac{\delta_m x}{\rho^k}\Big)\\ &= \delta_m x\frac{\log\frac{x}{x_3(m)}}{\log\rho}\log\rho + O\Big(\frac{\delta_m x}{\rho^k}\Big)\\ &= \delta_m x\log x - \delta_m x\log x_3(m) + O\Big(\frac{\delta_m x}{\rho^k}\Big)\\ &= \delta_m x\log x + O(x).\end{aligned}$$

Tudi za drugi člen si pomagamo z istim izrekom. Iz

$$\sum_{n\in I_j}\frac{1}{n} = \sum_{n\in(y_j,e^{\frac{\delta'_m}{2}}y_j]}\frac{1}{n} = \log\frac{e^{\frac{\delta'_m}{2}}y_j}{y_j} + O\Big(\frac{1}{y_j}\Big) = \frac{\delta'_m}{2} + O\Big(\frac{\rho^j}{x}\Big)$$

sledi

$$\begin{aligned}\sum_{j=1}^{k}\sum_{n\in I_j}\frac{1}{n} &= \frac{k\delta'_m}{2} + O\Big(\sum_{j=1}^{k}\frac{\rho^j}{x}\Big)\\ &= \frac{\delta'_m}{2} + \Big(\frac{\delta_m\log x}{8c_0} + O(1)\Big) + O(1)\\ &= \frac{\delta_m^2\log x}{128c_0} + O(1),\end{aligned}$$

pri čemer smo s pomočjo formule za vsoto vrste ocenili

$$\sum_{j=1}^{k}\frac{\rho^j}{k} = \frac{\rho(\rho^k-1)}{x(\rho-1)} < \frac{2\rho^k}{x} \le \frac{2}{x_3(m)} = O(1).$$

Tako imamo

$$\frac{\delta_m x}{2}\sum_{j=1}^{k}\sum_{n\in I_j}\frac{1}{n} = \frac{\delta_m^3 x\log x}{256c_0} + O(x).$$

Nadaljujemo

$$\begin{aligned}\sum_{n\le\rho^k}\frac{1}{n} &\le (\delta_m x\log x + O(x)) - \Big(\frac{\delta_m^3 x\log x}{256c_0} + O(x)\Big)\\ &= \Big(1 - \frac{\delta_m^2}{256c_0}\Big)\delta_m x\log x + O(x).\end{aligned}$$

Pripravili smo vse potrebno za oceno

$$\begin{aligned} |R(x)| &\leq \frac{1}{\log x} \sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right) \right| + o(x) \\ &= \left(1 - \frac{\delta_m^2}{256 c_0}\right) \delta_m x + o(x). \end{aligned}$$

Zdaj izberimo dovolj velik u_{m+1}, da za vsak $x \geq u_{m+1}$ velja

$$o(x) < \varepsilon_m \left(1 - \frac{\delta_m^2}{256 c_0}\right) \delta_m x.$$

Potem je

$$|R(x)| < (1 + \varepsilon_m) \left(1 - \frac{\delta_m^2}{256 c_0}\right) \delta_m x = \delta_{m+1} x.$$

Indukcija po m je končana in s tem je praštevilski izrek dokazan. □

Literatura

[1] M. B. Nathanson: *Elementary Methods in Number Theory*, Springer (2000).

[2] T. M. Apostol: *Introduction to Analityc Number Theory*, Springer-Verlag (1976).

[3] J. Bračič: *Uvod v analitično teorijo števil*, DMFA-založništvo (2003).

[4] D. Godfeld: *The elementary proof of the prime number theorem: An historical perspective*, preprint (1998).

[5] A. Granville: *On elementary proofs of the Prime Number Theorem for arithmetic progressions, without characters. In preceedings of the Amalfi Conference on Analityc Number Theory*, Universitá di Salerno (September 25-29, 1989), strani 157-195.